UNIVERSIDAD POLITÉCNICA DE MADRID

ESCUELA UNIVERSITARIA DE INGENIERÍA TÉCNICA DE TELECOMUNICACIÓN

INFRAESTRUCTURAS Y SERVICIOS DE TELEFONICA. IMPLEMENTACIÓN OFICINA MÓVIL BAJO EL SERVICIO VPNIP

Autor: Vicente García Ruiz
Director: D. Aurelio Berges García
Año: 2014

AGRADECIMIENTOS

Las primeras palabras de agradecimiento quería escribirlas para mi tutor Aurelio Berges García, por darme la oportunidad de llevar a cabo este proyecto de fin de carrera con él, apoyarme en la realización del mismo a pesar de largo periodo de elaboración que ha llevado este trabajo y por permitirme enfocar el proyecto con los criterios, la información y la experiencia recogida en mis años de trabajo en un operador de red como es Telefonica.

A todos mis compañeros "sufridores" de la universidad. Sé que han sido muchos años de esfuerzo y sacrificio pero todo tiene un final y este es el momento de terminar este largo trayecto. Ha sido un placer compartir grandes momentos con vosotros.

A mis compañeros de trabajo, por seguir apoyarme y asesorarme en algunos contenidos que en este proyecto se explican, en especial a Mario Montero López, cuya persona siempre ha tenido palabras de consuelo en mis momentos de desánimo y por aguantarme en los momentos de estrés cuando las cosas no iban como esperaba. Suerte en tu nueva andadura profesional, lo harás tan bien como siempre.

A mi pareja y alma gemela Lorena Prieto. Nadie mejor que tú para saber el enorme esfuerzo que me ha llevado hasta la consecución de este proyecto. Cuantas tardes y noches de trabajo aguantándome como la mejor y sabiendo que siempre te he tenido en los momentos que más te he necesitado. Siempre has sabido que tenía una espina clavada por no terminar la carrera debido a la falta de realización del proyecto. He sacado tiempo de donde no lo he tenido y ahora puedo decir que ya estoy a un pequeño de paso de ser Ingeniero. Gracias de corazón por estar siempre a mi lado y ser el motor de mi vida.

A mis amigos, sé que estáis muy orgullosos de que consiga final esta carrera. ¡Ya llega el momento de la presentación! Sabéis que no ha sido fácil compaginar la vida profesional con la vida de estudiante, pero con constancia, perseverancia y esfuerzo al final se consiguen los objetivos. Gracias a todos por estar ahí.

Por último, y como no podía ser de otra manera a mi familia. Siempre han tenido el sueño de tener un ingeniero en la familia. Los sueños que se persiguen y se desean con toda la fuerza, al final se cumplen. Abuela, me viste empezar la carrera pero las circunstancias de la vida no me han permitido que me vieras finalizarla. Estés donde estés este trabajo y título te lo dedico a ti. Siempre te llevo dentro de mí y ahora como no podía ser menos, apareces

en estas líneas. Espero que estés orgullosa de mí, siempre te querré. Mama, eres la verdadera productora de esta travesía y de que ahora mismo este aquí, ya que me has dado la oportunidad que tú no pudiste tener. Me has visto crecer como persona y dedicarle muchas horas a los estudios. Ahora es el momento nos veamos juntos celebrando el fin de esta etapa que tan duradera ha sido. Gracias mama por ser como eres y quererme como la que más.

Gracias a todos de corazón

RESUMEN

El presente proyecto de fin de carrera esta desarrollado para el explicar el estado actual de las telecomunicaciones en España. Mercado que esta en constante evolución tecnológica y que se ha pasado inicialmente medir por la tasa de penetración de líneas vocales en un país a pasar de hablar de indicadores como la voz IP, descarga de contenidos, uso de los dispositivos ya que el contenido de lo que las redes transporta es donde puede estar el negocio para los operadores.El proyecto de fin de carrera a groso modo está distribuido en dos partes.

La primera parte del proyecto, esta enfocado de una manera teórica haciendo una análisis del mercado actual de las telecomunicaciones. Para ello se realiza un primer estudio de los mercados de telecomunicaciones a nivel europeo y en España. Se analiza el sector de las TIC haciendo un repaso por los datos claves obtenidos en el último año y que han sido influenciados por la crisis mundial que vivimos en la actualidad. Detalles de la evolución de los servicios, infraestructuras de nueva generación desplegadas, inversiones y gastos de los operadores así como la cuota de servicio de los mismos. Regulaciones recientes e iniciativas como la Agenda Electrónica Digital para impulsar el crecimiento de la Sociedad de la Información. Investigación sobre la adopción y uso cotidiano de las nuevas tecnologías y dispositivos que hacen los ciudadanos que permiten mejoran nuestras vidas, la productividad de la economía y que será de devenir de las tendencias futuras hacia las que se moverá el mercado. Adicionalmente se plantea cuestiones sobre las tendencias de futuro de las redes de telecomunicaciones, analizando la previsión del volumen de datos creciente a transportar, los mecanismos para aumentar la capacidad, flexibilidad y eficiencia de las redes mediante técnicas como la virtualizacion (SDN).Debido a la experiencia profesional adquirida trabajando en un ISP como es Telefonica de España administrando sus redes y servicios a grandes empresas, profundizare con detalle técnico en estudiar y mostrar como estan montadas sus infraestructuras de red (Red IP Única, NGN, Multiservicio/UNO,…) , los diferentes tipos de accesos a las redes incluyendo los de nueva generación (FTTH) así como el catalogo de servicios ofertados (Macrolan, VPN-IP, Ibercom IP…), principalmente basados RPVs y sus facilidades asociadas sobre las mencionadas redes para las grandes empresas, PYMES y residencial que les permite la comunicación nacional o internacional entre las diferentes emplazamientos de sus oficinas con sus sedes centrales.

La segunda parte de este proyecto se describe la implementación de un caso práctico real tanto en tema de configuración y montaje de equipamientos empleados (router,antena 3G…) de una oficina móvil basado en el servicio vpn-ip de Telefonica con acceso móvil 3G que se encuentra en el actual portfolio de sus productos que se explico en teóricamente en la primera parte del proyecto y que tiene conectividad con la red IP Única de la RPV del cliente Caja de Seguros Reunidos (CASER) la cual que nos permitirá conectarnos remotamente a un servidor de monitorización de su intranet ubicada en su sede central de Madrid que muestreara el trafico que se esta cursado por los interfaces del router de la oficina móvil. En la configuración del router se empleara diferentes métodos de conectividad como túneles GRE para la conectividad con los equipos de la red IP Única, LT2P y PPP para el acceso a la red móvil y se dotara de mayor seguridad al trafico cursado por la oficina Mobil empleando túneles IPSEC para la encriptación y cifrado de los datos para evitar que el trafico que va en claro por la red móvil si es interceptado por un tercero no sea capaz de analizarlo y descifrarlo y no se vea afectada la privacidad de la información que estamos transmitiendo.

ÍNDICE

INTRODUCCIÓN

El mercado de las telecomunicaciones ha evolucionado y evoluciona muy rápidamente y más en los tiempos difíciles que nos esta tocando vivir. Con el paso del tiempo hemos **pasado de poner el foco de atención sólo en la infraestructura** y los terminales de los primeros años, tecnología que ya está a nuestra disposición**, a centrar el análisis en la adopción y uso cotidiano de las nuevas tecnologías** para mejorar nuestras vidas y la productividad de la economía. Si hasta los años ochenta del siglo XX la implicación de las telecomunicaciones en la economía se medía por la tasa de penetración de líneas vocales en un país ahora se tienen en cuenta también otros indicadores.

Dichos indicadores nos hablan del comercio electrónico, de los accesos a Internet, de las empresas que lo tienen como herramienta o las que lo utilizan como base de su negocio. Ni siquiera se habla de las redes IP, sino de la voz sobre IP, de las descargas a través de la red. Es decir, se habla directamente del nivel más alto de la escala de creación de valor. Las **operadoras de telecomunicación** que en el pasado **creaban y gestionaban redes de transporte** ahora tienen que tener en cuenta lo que esas redes transportan o **pueden transportar porque es ahí donde está el negocio.**

Las telecomunicaciones siempre han estado presentes en los negocios, pero eran una parte, una herramienta más que permitía su desarrollo y que facilitaba las cosas. La situación desde los años noventa ha cambiado radicalmente. Ahora están en el corazón del negocio y de sus prestaciones dependen la viabilidad o no de las empresas. Las telecomunicaciones mismas han pasado de ser un buen negocio, pero pesado, lento en retornos, un negocio de infraestructura, a ser, en alguna de sus variantes, un negocio ágil, de ganancias rápidas, de mercados masivos y dinámicos. De ahí su encanto y de ahí sus riesgos.

Estamos viviendo revoluciones como la de Internet y los móviles simultáneamente, cada una con capacidad por sí misma para transformar la sociedad y la economía. Hoy somos una sociedad más informada, con mejor acceso al conocimiento y con una mayor interacción social. A estas dos revoluciones básicas se han unido las de la banda ancha fija, la banda ancha móvil, los buscadores de Internet, las redes sociales y los dispositivos inteligentes móviles como los smartphones y las tabletas.

La crisis global, con efectos notables en nuestra economía, ha provocado **una pérdida de confianza y elevadas tasas de desempleo** y ha dificultado el acceso al crédito, lo que ha comprometido la continuidad de muchas empresas. Estos factores, que impactan directamente en **la caída del consumo**, no parecen haber hecho mella en la penetración de Internet móvil, que goza de una envidiable salud en España como servicio de alto valor añadido. En la actual coyuntura económica el camino adecuado para poder **superar esta situación de crisis** es adoptar de manera inteligente tecnologías digitales que permitan **desarrollar modelos económicos productivos y eficientes** en los que la **innovación tecnológica** sirva de motor del crecimiento y del incremento de la productividad.

OBJETIVOS Y MOTIVACIONES

Como amante y apasionado de las nuevas tecnologías, dispositivos y en especial de las redes de telecomunicaciones que por fortuna en la actualidad me estoy dedicando a ellas profesionalmente y cada día con más ganas de aprender y afrontar nuevos proyectos que me permitan crecer profesionalmente y como persona asumiendo nuevas responsabilidades las motivaciones que me llevaron a la realización de este proyecto ha sido la investigación sobre cómo han evolucionado las redes de comunicaciones que han sentado los principios de las redes que conocemos, es más, dichas redes como la red UNO o servicios como Iberpac que ya parecen obsoletos, en la actualidad, aunque no se comercionalizan, si son todavía utilizados por los ciertos clientes ya que el software o equipamiento que existe detrás de una X.25 para migrarlo a IP conlleva tal complejidad que no es cosa de un día migrar ciertos tipos de servicios, al igual que las RPVs de N2 o tradicionales. Conocer el mercado y como están evolucionando los servicios y tecnologías era una motivación adicional para entender lo que está por venir, como la virtualización. Pero añadir que la principal motivación que tenía para realizar este proyecto es analizar los servicios e infraestructuras del operador Telefonica ya que su estudio me iba a permitir conocer con detalle sus redes pudiendo desarrollar y ejecutar mejor mi trabajo como Ingeniero de Explotación de Telefonica para el gran cliente Caser, tanto en el diagnóstico y tratamiento de averías como para permitir una mejor asesoramiento a los clientes sobre las ventajas, inconvenientes y funcionamiento de los servicios que tienen contratados con Telefonica.

Respecto a los objetivos que he buscado en la elaboración de este proyecto son numerosos ya que he tratado de conocer e informar tanto el estado de los servicios y redes actuales y lo

que está por venir. A continuación paso a describir los objetivos que se pretende alcanzar con este trabajo.

- Dar a conocer **el estado actual del mercado de las telecomunicaciones tanto en el mundo, viendo las economías emergentes, en Europa como en España**. Se enfoca desde el punto de vista de la Sociedad de la Información y las TIC. Para ello se pretende indicar como están los servicios como la telefonía fija, móvil, la banda ancha y los servicios mayoristas mediante gráficas y comparativas de años anteriores para entender cómo se está desarrollando el mercado. Inversiones, facturación y gastos realizados por los operadores. Cuota de mercado de los mismos.
- **Analizar el uso que dan los ciudadanos a las tecnologías**. Penetración de internet en los hogares, dispositivos más utilizados para navegar. Información consultada a la hora de navegar. Métodos de comunicación y mensajería instantánea preferidos por los usuarios. Tipos de compras realizadas por internet así como sus métodos de pago. Por último, las redes sociales utilizadas analizadas en función de la edad del internauta.
- Investigar sobre **el futuro de las redes y las tecnologías**. Tendencias que están llegando como la virtualización, el internet de las cosas y la era de todo conectado.
- Mostrar una **visión detallada de la estructura de las redes y servicios basados en RPVs del operador Telefonica**. Describir y analizar con precisión como está montada y diseñadas las redes de Telefonica, tanto las de acceso como las de backbone o transporte. Servicios ofertados a grandes cuentas y PYMES para el transporte de información e interconectar sus delegaciones. Facilidades que ofrecen los servicios y requisitos que deben cumplir los clientes en sus comunicaciones.
- **Enseñar el funcionamiento del servicio vpn-ip de Telefonica con acceso móvil 3G**. Para ello se pondra en marcha con equipamiento real (router, antena 3G…) la simulación de una oficina remota que intenta acceder a un servidor de la intranet de una Empresa (Caser) ubicado en Madrid haciendo uso de la red IP Unica de Telefonica entre otras.

ORGANIZACIÓN DEL CONTENIDO DEL PROYECTO

El extenso proyecto que ahora me ocupa tiene su contenido distribuido en diferentes capítulos en dos partes tal y como explique en el resumen los cuales paso a resumir su información tal y como índico a continuación:

*** Introducción:** En este apartado se realiza una breve introducción del contenido del proyecto junto los objetivos y las motivaciones que han llevado a la realización de este trabajo. Adicionalmente se indica como está distribuido en contenido de la información que he tratado de explicar a lo largo de las siguientes páginas.

*** La Parte 1 del proyecto:** contiene el estudio teórico del mercado actual de las telecomunicaciones en materia de líneas, servicios y cuota de mercado de los diferentes operadores que prestan su servicio en España así como las tendencias y usos que se le dan a las diferentes tecnologías por parte de la ciudadanía. Se mostrara como están montadas las redes del operador Telefonica, los servicios de RPVs que ofrece empleando dichas infraestructuras. Esta parte de complemente de un documento anexo (memoria_anex.pdf) el cual contiene toda la información mas técnica referente a protocolos, tipos de accesos, equipamientos de las redes para liberar de carga teórica esta memoria. Esta parte esta desglosada en los siguientes capítulos:

- **Capítulo 1. Contexto actual de las telecomunicaciones:** Introducción de la situación actual del mercado de las telecomunicaciones enfocándolo brevemente desde el punto de vista de la Sociedad de la Información y de las TIC.
- **Capítulo 2. Indicadores más significativos:** Se analiza los sucesos importantes que han acontecido en el año 2012 en España en materia económica (inversiones y facturación), los servicios (banda ancha y Smartphone), regulaciones y nuevos servicios como NEBA.
- **Capítulo 3. Sector de las telecomunicaciones en el contexto europeo:** En este caso se indica los objetivos y actuaciones de la agenda digital europea para el mercado de las telecomunicaciones. Se detalla el mercado por servicios, explicando cada uno de ellos y los esfuerzos económicos en TI realizado por los operadores.
- **Capítulo 4. Sector de las telecomunicaciones en el España:** Para entender la evolución de los servicios en España, se analizan los mismos (telefonía fija y móvil, banda ancha fija y móvil, infraestructuras y servicios mayoristas) en temas como el

número de líneas, ingresos, tráfico y cuota de mercado de los operadores que permitirá dar un visión detallada de cómo está el mercado en España. Adicionalmente se menciona el mercado de grande cuentas o clientes donde Telefonica sigue siendo el rey indiscutible.Se estudia adicionalmente las tendiencias y el uso que dan los ciudadanos a las tecnologías y dispositivos, así como el tipo de información que acceden y los métodos preferidos para comunicarse. Mencion al comercio electronico y el uso de las redes sociales.

- **Capítulo 5. Futuro de las redes y la tecnología:** Análisis de la previsión del crecimiento de los datos en la era de la información que estamos viviendo. Técnicas para ese transporte masivo de los datos como son las mallas fotónicas y las small cells. Virtualización de las redes (SDN) y uso de las mismas
- **Capítulo 6. Estructura de red y servicios del operador Telefonica:** Este es el capítulo más extenso y técnico de todo el proyecto. El trabajar en la actualidad para Telefonica y la experiencia adquirida durante estos años me permite explicar con detalle cómo están montadas las redes, sus arquitecturas así como los servicios que se están ofertando en la actualidad a grandes clientes y PYMES. Se analiza la red IP Única, UNO, NGN en profundidad, así como los servicios que se están ofertando sobre las mismas con sus características y facilidades. Las redes de acceso fijo, como la red 50, Alejandra, GigADSL y MAN son estudiadas con detenimiento, al igual que las redes de acceso móvil GSM/UMTS y LTE.

*** La Parte 2 del proyecto:** se muestra un caso práctico del funcionamiento real del servicio vpn-ip de Telefonica que emplea la red IP Única para tener acceso a equipamientos remotos de la sede central del cliente Caser que ha mostrado su colaboración para este proyecto. Se compone del siguiente capitulo:

- **Capítulo 1. Descripción general de la solución:** Se explica en que va a consistir el montaje de la oficina móvil empleando el servicio vpn-ip con acceso 3G de manera general sin hacer entrar en detalles específicos de configuraciones y protocolos.
- **Capítulo 2. Equipamiento empleado en la oficina móvil:** Se detalla los elementos que intervienen (router, antena 3G, adaptador POE…) para hacer funcionar la oficina móvil así como sus características técnicas.

- **Capítulo 3. Parámetros de provisión para configurar el router:** En este capitulo se incluye los parámetros que se han de configurar en el router para tener conectividad con la sede central de Caser. Dichos parámetros son las IPs de los interfaces, contraseñas, vlanes, usuarios y otra serie de datos.
- **Capítulo 4. Esquema y explicación detallada de la infraestructura global:** Esquema detallado con las IPS que de todos los elementos que intervienen en la red, los túneles GRE e IPSEC y su funcionamiento detallado.
- **Capítulo 5. Configuración router 887 oficina móvil:** Este apartado se explica los comando que se deben configurar en el router cisco 887 para montar los túneles GRE con los POI, el túnel IPSEC, la vlan de la LAN, el túnel L2TP e interfaz PPP para la gestión de la antena y el routing BGP para la tabla de rutas.
- **Capítulo 6. Configuración router oficina central:** Incluye los comandos a introducir en el router central para montar el túnel IPSEC con la oficina remota y los comando para configurar el routing dinámico y anunciar hacia la red IP Única la red 10.11.43.0/24 donde se encuentra el servidor de monitorización.
- **Capítulo 7. Pila de protocolos que intervienen en la solución:** Esquema con los protocolos que intervienen en el funcionamiento de la oficina móvil, la explicación, interaccion y dependencia entre cada uno de ellos.
- **Capítulo 8. Troubleshooting para comprobar el funcionamiento:** En este último apartado se incluye los comandos, las trazas obtenidas del router y pruebas de conectividad para comprobar que la vpn-ip funciona correctamente y que el servidor de monitorización muestrea el tráfico del router.

*** Conclusiones:** Se exponen las conclusiones que he alcanzado tras la realización de este proyecto para ambas partes y que me han permitido conocer con detalle el mercado, las infraestructuras de redes y servicios de Telefonica así como el funcionamiento real de uno de sus servicios vpn-ip que comerciliza en la actualidad.

*** Bibliografía:** Detalla las fuentes de información usadas en la elaboración del presente proyecto tanto para la parte 1 como la parte 2.

PARTE 1: ANÁLISIS DEL MERCADO DE LAS TELECOMUNICACIONES EN ESPAÑA. REDES Y SERVICIOS ACTUALES DE TELEFONICA

1 CONTEXTO ACTUAL DE LAS TELECOMUNICACIONES

Las telecomunicaciones siempre han estado presentes en los negocios, pero eran una parte, una herramienta más que permitía su desarrollo y que facilitaba las cosas. La situación desde los años noventa ha cambiado radicalmente. Las telecomunicaciones mismas han pasado de ser un buen negocio, un negocio de infraestructura, a ser, en alguna de sus variantes, un negocio ágil, de ganancias rápidas, de mercados masivos y dinámicos.

No es fácil vivir en una misma generación revoluciones como la de Internet y los móviles simultáneamente, cada una con capacidad por sí misma para transformar la sociedad y la economía tal y como se analizó anteriormente llegando a la **creación del movimiento de la Sociedad de la Información.**

El reto para los individuos que se desarrollan en todas las áreas de conocimiento es vivir de acuerdo con las exigencias de este nuevo tipo de sociedad, estar informados y actualizados, innovar, pero sobre todo **generar propuestas y generar conocimiento**, conocimiento que surge de los millones de datos que circulan en la red. El **fenómeno de la Sociedad de la Información se refiere a grandes rangos a todos aquellos sectores que permanecen por muy diversas razones, al margen de los beneficios y ventajas asociados a las TIC** (Tecnología de la Información y Comunicación).

Más allá del papel que las tecnologías tienen para el futuro económico y desarrollo competitivo de los países, estas son modificadores básicos de la sociedad, en su cultura y en sus hábitos, incluso de su manera de ver el mundo. Las TIC llevan ya décadas realizando esta transformación. Hoy somos una sociedad más informada, con mejor acceso al conocimiento y con una mayor interacción social. A estas dos revoluciones básicas se han unido las de la banda ancha fija, la banda ancha móvil, los buscadores de Internet, las redes sociales y los dispositivos inteligentes móviles como los smartphones y las tabletas .Para conseguir esta **innovación tecnológica** han unido sus esfuerzos los operadores de telecomunicaciones, los suministradores de equipos, los desarrolladores de software y los proveedores de servicios en Internet. Todos estos componentes son esenciales y, por tanto, han de encontrar un modelo económico sostenible en esta nueva etapa. Hoy, la adopción

de las TIC por parte de la sociedad en la vida cotidiana y de la economía en general, supone avances y transformaciones.

Si hay un **sector que se caracterice por su esfuerzo innovador y por su potencial** para transformar la realidad, ése es el macrosector de **las Tecnologías de la Información y las Comunicaciones**. La creación de nuevos productos y servicios TIC habilita a su vez el desarrollo de múltiples ámbitos y sectores económicos, facilita nuevos modelos de negocio, reduce barreras de entrada, multiplica la productividad, impulsa el crecimiento…en definitiva, añade un fuerte valor al conjunto de la sociedad. **España es ya una Sociedad en Red**, pero la adopción de las TIC por parte de la sociedad y de la economía en general sigue siendo un reto y por eso requiere de una supervisión y análisis periódicos para buscar el modo más eficiente de impulsarlo.

Con el paso del tiempo hemos **pasado de poner el foco de atención sólo en la infraestructura** y los terminales de los primeros años, tecnología que ya está a nuestra disposición**, a centrar el análisis en la adopción y uso cotidiano de las nuevas tecnologías** para mejorar nuestras vidas y la productividad de la economía. Si hasta los años ochenta del siglo XX la implicación de las telecomunicaciones en la economía se medía por la tasa de penetración de líneas vocales en un país como he analizado anteriormente en las primeras fases del proyecto, ahora hay que tener en cuenta más indicadores.

Dichos indicadores nos hablan del comercio electrónico, de los accesos a Internet, de las empresas que lo tienen como herramienta o las que lo utilizan como base de su negocio. Ni siquiera hablaremos de las redes IP, sino de la voz sobre IP, de las descargas a través de la red. Es decir, hablaremos directamente del nivel más alto de la escala de creación de valor. Las **operadoras de telecomunicación** que en el pasado **creaban y gestionaban redes de transporte** ahora tienen que tener en cuenta lo que esas redes transportan o **pueden transportar porque es ahí donde está el negocio**.

La crisis global, con efectos notables en nuestra economía, ha provocado **una pérdida de confianza y elevadas tasas de desempleo** y ha dificultado el acceso al crédito, lo que ha comprometido la continuidad de muchas empresas. Estos factores, que impactan

directamente en **la caída del consumo**, no parecen haber afectado en la penetración de Internet móvil, que goza de buena salud en España como servicio de alto valor añadido. En la actual coyuntura económica todos los expertos apuntan a que el camino adecuado para poder **superar esta situación de crisis** es adoptar de manera inteligente tecnologías digitales que permitan **desarrollar modelos económicos productivos y eficientes** en los que la **innovación tecnológica** sirva de motor del crecimiento y del incremento de la productividad.

Que la comunicación sea un elemento en constante crecimiento nos hace pensar que la nueva etapa económica que se iniciará tras la superación de la crisis, tendrá a las TIC y al mundo digital en el núcleo de su construcción. Los operadores de telecomunicación, las ya empresas digitales como Telefónica, han sido uno de los protagonistas de toda esta evolución. Los operadores digitales van a ser protagonistas esenciales en la próxima etapa, cuyos cimientos se están construyendo a partir del **despliegue de tecnologías claves como la cuarta generación de telefonía móvil, el denominado LTE**, o la fibra hasta el hogar, que ha multiplicado el número de líneas casi por 2 en España en tan solo un año. Entramos en la segunda etapa de evolución del mundo digital, en la que son tan importantes las infraestructuras como los dispositivos, servicios o aplicaciones.

La crisis ha puesto de manifiesto algo bien consabido a lo largo de la historia: las potencias industriales han demostrado ser más resistentes que los países con insuficiente base industrial. **Siendo innovadores, pioneros y competitivos, más esforzados e imaginativos podremos seguir disfrutando de un "estado de bienestar"**. En **España, la recuperación** está siendo **más lenta** como consecuencia del gigantesco **impacto de la burbuja inmobiliaria**, su tardío y todavía insuficiente reconocimiento por el sistema financiero, déficit públicos excesivos e incontrolados, ausencia de reformas estructurales que posibiliten un crecimiento. El desempleo, con tendencia a convertirse en algo muy preocupante, afecta a una proporción de la sociedad española que, en el caso de los jóvenes, alcanza niveles literalmente vergonzosos y de emergencia nacional.

Sin embargo, nuestro país se encuentra felizmente instalado en una de las regiones del planeta con mejor calidad de vida y con un nivel de conocimientos extraordinario, que se acaba de dotar de una Agenda Digital como base de la recuperación de su competitividad y

liderazgo internacional. Dicha Agenda asume que nuestro futuro está relacionado con la posibilidad de constituirnos como una potencia industrial de la nueva era económica, competitiva, sostenible y capaz de generar un alto valor añadido que posibilite mantener y acrecentar el nivel y estilo de vida que hemos elegido.

2 INDICADORES MÁS SIGNIFICATIVOS

Los indicadores observados en el sector de las telecomunicaciones en España durante 2012 fueron similares a las experimentadas en el resto de los países de la Unión Europea. Por un lado, y a pesar de la crisis económica, **aumentó la penetración de los servicios**, excepto el de telefonía fija, y se incrementó el consumo. Por otro, se **redujeron los ingresos por prestación** de la mayoría de los servicios finales, aumentando únicamente los relativos a la banda ancha móvil.

2.1 LA BANDA ANCHA MÓVIL SUPONE EL CRECIMIENTO DE LA BANDA ANCHA EN ESPAÑA

La demanda de banda ancha en España ha **seguido creciendo durante el año 2012 a pesar de la crisis**. Las líneas de **banda ancha móvil registraron un significativo aumento, del 44,2%, hasta alcanzar los 24,9 millones** de líneas llegando a una **tasa de penetración de 54 líneas por cada 100 habitantes**. Un total de 19,3 millones de líneas móviles accedió a Internet a través de las redes para comunicaciones móviles, lo que supuso un aumento de la demanda vinculada a estos servicios del 65,5%. La mayoría de conexiones de banda ancha móvil, un 82,5%, se realizaron con terminales de voz.

2.2 LA BANDA ANCHA MÓVIL SUPERA A LA ANCHA BANDA FIJA

Este año también se ha producido otro cambio importante: **el ratio líneas por habitante de la banda ancha móvil ha superado al ratio de la banda ancha fija en España**. Así, las penetraciones de banda ancha fija y móvil fueron, respectivamente, de 24,9 y de 54 líneas por cada 100 habitantes tal y como se comento anteriormente. Este espectacular crecimiento de la banda ancha móvil tiene su origen en el uso de teléfonos inteligentes, tabletas y otros dispositivos similares.

2.3 DESCIENDE EL NÚMERO DE LINEAS MOVILES POR PRIMERA VEZ

La telefonía móvil **perdió 2.766.465 líneas en 2012**, lo que **supone el 4,9%** menos que en 2011 y la primera caída de su historia. Por operadores, en el conjunto del año, Movistar perdió 3,1 millones de líneas y Vodafone restó un total de 1,6 millones de líneas. Por el contrario, los **Operadores Móviles Virtuales (OMVs) ganaron un total de 1,2 millones de líneas**, Yoigo sumó 493.405 líneas y Orange 72.775 líneas. Esta cifra, que se obtienen de sumar los datos aportados mes a mes por la CMT. Destacar que **5,23 millones de números móviles cambiaron de operador en el año**, una cifra ligeramente inferior a los 5,58 de hace un año.

2.4 SMARTPHONE SUPERA AL PC COMO DISPOSITIVO MAS VENDIDO EN EL MUNDO

Este año, los titulares y casi todo el protagonismo se lo ha llevado un dispositivo, **el smartphone**. Los teléfonos inteligentes, y las tabletas, llevan cambiando nuestros hábitos de consumo de Internet desde hace 4 años. **Este año han superado las ventas de PC** en el segundo trimestre y lo que era impensable, la facturación en juegos para estos dispositivos ha superado la facturación de las consolas. Su existencia ha **disparado el consumo de datos en el móvil y la banda ancha en el móvil** ha superado a la banda ancha fija. Además, **España es con el Reino Unido el líder en porcentaje de estos dispositivos dentro de su parque de móviles con más del 46,3% del total**. Además, el incremento espectacular en las líneas de Internet móvil en España está directamente relacionado con el uso de smartphones, que suponen ya el 57% de los teléfonos móviles en España, situando a **nuestro país como uno de los países con un parque de telefonía móvil más avanzado del mundo.**

2.5 SIGUE DECRECIENDO EL NEGOCIO DE LAS COMUNICACIONES TRADICIONALES

Tal y como se percibe la tendencia de los últimos años, **las comunicaciones tradicionales como es la telefónica fija y los SMS siguen su descenso** debido a las nueva modalidades de comunicación. Así, durante el 2012, el Teléfono fijo registró un descenso del 10,7% frente al 7,9% del año anterior en materia de ingresos. El **número de líneas de**

telefonía fija en servicio fue de 19,9 millones, **350000 líneas menos que el año anterior**. Las líneas fijas residenciales y de negocios registraron pérdidas de líneas.

Los SMS y MMS han presentado reducciones de tráfico en los últimos ejercicios. En concreto, en 2012 el tráfico de mensajes SMS entre abonados (excluidos los SMS de valor añadido) disminuyó un 6,1%. Fue el cuarto año consecutivo en el que se registra una caída del tráfico de este servicio. **Todo esta reducción de cifras es debido al auge del incremento de los servicios de mensajería por internet como es el Whatsapp y las redes sociales tipo Facebook**, estas últimas son utilizados por el 54,1% de los jóvenes tras una subida de 19 puntos porcentuales, y se coloca como el tercer canal de comunicación entre los jóvenes tan solo por detrás del teléfono móvil que es usado por el 94,1% de ellos y por la comunicación en persona que utiliza el 65,5%.

2.6 AUMENTO DE LAS REDES NGA

Los **operadores han invertido en mejoras las redes NGA (New Generation Access)** y redes híbridas de cable y coaxial con la implementación de la tecnología bajo el estándar DOCSIS 3.0, que permite al cliente final contratar ofertas de velocidades de 50 o de 100 Mbps. A finales del ejercicio, el total de accesos de **HFC habilitados con esta tecnología alcanzó los 9 millones, lo cual supone el 95,3%** del total de accesos de las redes HFC.

De entre todas las alternativas de acceso disponibles, la que **mayor potencial de crecimiento** es la que utiliza fibra óptica en la totalidad de la red incluyendo el tramo final de acceso al hogar, la llamada "fibra hasta el hogar" **o FTTH**. **La fibra óptica ha tenido un crecimiento** más espectacular, **por encima del 210%** durante el último año, con un total de 1,6 millones de accesos instalados, principalmente realizados en las ciudades más pobladas (Madrid, Barcelona, Valencia…), aunque todavía posee una penetración muy baja y cuenta con una cuota de mercado del 1%.

2.7 FIRMA ACUERDO PARA OFRECER EL SERVICIO NEBA

En anteriores aparatados se hizo referencia a la oferta de acceso al bucle de abonado (OBA) aprobado por Real Decreto de Reglamento para facilitar la liberación del mercado y la oferta de servicios a otros operadores que no tienen red propia. **La CMT fija las condiciones en las que Telefónica, como operador con poder significativo en el**

mercado, debe poner a disposición de otros operadores determinados elementos de su red. Estos servicios mayoristas que Telefónica está obligada, a prestar quedan recogidos en la **Oferta de Acceso al Bucle de Abonado** de este operador, que es aprobada por la CMT. La poca diferenciación que permiten los servicios mayoristas de acceso indirecto actuales con respecto a las ofertas de Telefónica motivó sacar al mercado, en 2011, de un **nuevo servicio de acceso indirecto (Nuevo Servicio Ethernet de Banda Ancha, NEBA).** Este servicio, que sustituirá progresivamente al GigADSL y al ADSL-IP, facilita el **acceso mayorista a la nueva red de fibra de Telefónica basado en Ethernet y permite ofrecer servicios de mayor valor añadido** con garantías de calidad para prestar telefonía IP aplicando mecanismos de calidad de servicio. **Para más información del servicio NEBA consultar el documento memoria_anex.pdf apartado ANEXO1.**

2.8 TELEFONICA: CUOTA DE MERCADO POR DEBAJO DEL 50%

Lo que parecía imposible hace tan solo cuatro años ha ocurrido. La **fuga de clientes de Telefónica** hacia otros operadores producida mes a mes desde que se inició la crisis, ha producido un vuelco histórico desde la llegada del ADSL a nuestro país**.** La presión constante durante los últimos cuatro años de los operadores alternativos ha **acabado por destronar a Telefónica** de su lugar histórico como operador con la mayoría absoluta de clientes. La erosión mes a mes que suponen las portabilidades desde el exmonopolio hacia otros operadores hace notar en la cuota de mercado de la banda ancha. **Telefónica reduce su porcentaje de mercado al 49,64**%. Se trata de la primera ocasión, desde que la banda ancha llegó a nuestro país en 1999**,** que Telefónica baja del 50%. Esto significa que por primera vez los operadores alternativos reúnen más clientes que Telefónica.

Por el contrario, cabe **destacar que Telefonica se esta asegurando el futuro en la banda ancha basado en la tecnología FTTH**, ya que como se ha comentado antes, esta haciendo un despliegue de fibras que ha supuesto un **crecimiento de un 227%** respecto hace un año.

En la telefonía móvil el resultado también ha supuesto un duro batacazo, ya que se **registró la mayor cifra de portabilidades de la historia de la telefonía móvil en España**. Los **Operadores Móviles Virtuales (OMV)** fueron quienes lideraron el mercado, ya que **acapararon más de dos tercios del total de altas netas** de la telefonía móvil.

2.9 OFERTA INTEGRADA DE SERVICIOS

El año 2012 estuvo marcado por la aparición de ofertas comerciales con un mayor número de servicios tanto móviles como fijos. Debido a la pérdida masiva de clientes por parte de Telefónica y con la cuota de mercado analizada anteriormente, esta última ha decidido sacudir el mercado con una **oferta que integra telefonía fija, móvil, banda ancha** (ADSL o fibra) y televisión, con una **factura única** para el cliente suponiendo un **ahorro de hasta un 50%** conocida como Movistar Fusión.

Esta oferta realizada por Movistar, ha supuesto que el resto de operadores de telecomunicaciones (Vodafone, Jazztel, Ono), para tratar de competir con la oferta de Movistar, que también estén empaquetando todos los servicios en una misma factura suponiendo al cliente un ahorro en el importe a pagar y buscando una fidelización y compromiso en los servicios contratados por los clientes para que todos los servicios estén con el mismo operador de telecomunicaciones.

Así, a las ofertas de banda ancha y voz fijas, que son los paquetes más numerosos en el mercado, se sumaron los servicios la banda ancha móvil y voz móvil de modo empaquetado**. Estos paquetes cuádruple play representaron el 10,5% del total de líneas de banda ancha** y 146.132 paquetes con cinco servicios, que añaden la televisión de pago al resto de servicios. Por otra parte, se observaron reducciones de los precios efectivos en los paquetes más contratados, lo que supone **que el gasto medio del hogar que contrata estos servicios se redujo un 6,9%**.

2.10 DISMINUCIÓN DE LA FACTURACIÓN GLOBAL DEL SECTOR

En el contexto de crisis económica que se encuentra el país, el sector de las telecomunicaciones no iba a mantenerse al margen de caída del consumo, por ello, la **facturación global del sector** fue de unos 38000 millones de euros, lo que supuso **una disminución del 4,6%** con respecto al año anterior. Tanto los servicios finales como los mayoristas alcanzaron unos niveles de facturación inferiores a los registrados un año antes (-5,3% y -1,2% respectivamente). **El único servicio minorista cuyos ingresos aumentaron fue el de banda ancha móvil, que registró un incremento del 23,5%.**

2.11 CAÍDA DE LA INVERSIÓN

La inversión del sector realiza por los operadores descendió un 8,9% respecto al año anterior de 3.971,1 millones de euros en 2012 frente a 4.358,6 millones de euros en 2011, todo ello, sin tener en cuenta las inversiones realizadas por los operadores en el espectro radioeléctrico.

2.12 NUEVA LEY GENERAL DE TELECOMUNICACIONES

En el pasado Consejo de Ministros del **13 de septiembre de 2013 se ha aprobado el Proyecto de Ley General de Telecomunicaciones.** La Ley actualiza la normativa para adaptarla a los profundos avances que ha vivido el sector de las telecomunicaciones y para favorecer el desarrollo futuro de la economía digital, que el Gobierno considera uno de los motores principales económicos con más potencial de crecimiento en España.

El Proyecto de Ley actualiza la normativa vigente que data de 2003 y resuelve determinadas cuestiones que afectaban negativamente a la competitividad de los operadores de telecomunicaciones, como lo son la penalización del despliegue de nuevas redes, la inversión y la provisión de servicios. Por su parte, los usuarios verán mejoras en la cobertura, un incremento de la velocidad de Internet y la reducción de precios y costes. Además, se mejora la protección al usuario. **La ley** introduce reformas estructurales en el régimen jurídico de las telecomunicaciones, **con dos objetivos principales**:

- **Facilitar el despliegue de redes de nueva generación**, tanto fijas como móviles, ampliando su cobertura reduciendo los costes para que pueda redundar en el precio final que pague el usuario.
- **Mejorar la oferta de servicios innovadores a los ciudadanos**, de mayor calidad y a unos precios más asequibles, impulsando unas condiciones más efectivas de competencia.

Para conseguir los objetivos que persigue la ley, **las medidas que propone la ley** para llevarlos a cabo van encaminadas sobre 4 directivas:

1. **Impulsar la competencia y mejorar los servicios de los usuarios**. Para ello se tomaran medidas que analicen periódicamente el mercado, se supervisara las actuaciones de las administraciones publicas sobre las redes y se mejorara los derechos de los usuarios y su protección de datos.

2. Intentar **recuperar la unidad del mercado y la separación normativa**. Se proponen nuevas actuaciones de colaboración entre el estado y las Comunidades Autonómicas. Las redes son de interés general por lo que se obliga a la instalación de las mismas en nuevas zonas de urbanización y con requisitos técnicos comunes a nivel nacional.
3. **Simplificar los trámites administrativos**. Se propone que la gestión del acceso al espectro sea más fácil y que se suprima las licencias medioambientales y urbanísticas en el despliegue de las redes.
4. **Facilitar la instalación de las redes**. Para que los usuarios tengan derecho al uso de redes ultrarrápidas, a los operadores se les va a permitir reutilizar infraestructuras de los edificios, como canalizaciones, conductos o emplazamientos de titularidad pública para que las obras suponga una menor inversión y ello redunde en beneficio de los ciudadanos.

Los impactos que tendría en la economía, junto con el cumplimiento de la Agenda Digital, según estudios de la Comisión Europea, supondría que un incremento del 10% en la penetración de la banda ancha con lleva un **crecimiento del PIB de entre el 1% y 1,5%**. Además, según estos estudios, duplicar la velocidad de la banda ancha en una economía supone un incremento **del 0,3% del PIB y la inversión en los nuevos servicios generaría la creación de nuevos puestos de trabajo.**

3 SECTOR DE LAS TELECOMUNICACIONES EN EL CONTEXTO EUROPEO

Si bien **la crisis económica** afectó de **modo diferente a los distintos países de la UE**. Así, **aumentó** la penetración de los servicios más relevantes**,** como **el de móvil, el de banda ancha y el de televisión** de pago, mientras que **descendió la facturación global** en el conjunto de la UE. El motor del sector fueron los servicios de datos en movilidad, con un crecimiento muy importante. Los Gobiernos de los países miembros de la UE han adoptado **políticas para impulsar la Sociedad de la Información** y los operadores han realizado un esfuerzo en la extensión de las redes 3G-UMTS y el **despliegue de las redes LTE**.

En un contexto de salida muy lenta de la **crisis económica y estando en recesión**, los operadores **reaccionaron disminuyendo los precios**. La zona euro registró un **crecimiento negativo del 0,5%.** En cualquier caso, se espera que el **sector crezca a tasas inferiores a las del PIB,** tal y como viene sucediendo en los últimos años.

Por otra parte, La Comisión Europea puso en marcha en marzo de 2010 **la Estrategia Europa 2020**, con el claro **objetivo de salir de la crisis y preparar a la economía** de la UE para los retos de la próxima década. Europa 2020 expone una estrategia que debe aplicarse a través de medidas concretas encaminadas a conseguir niveles elevados de empleo y una economía de mejora de la productividad. La **Agenda Digital** para Europa es una de las iniciativas genéricas dentro de la Estrategia cuyo propósito es obtener los **beneficios económicos y sociales sostenibles que pueden derivar de un mercado único digital** basado en una Internet ultrarrápida.

3.1 OBJETIVOS DE LA AGENDA DIGITAL

3.1.1 Banda ancha

- **Banda ancha básica para todos en 2013:** cobertura de banda ancha básica para el 100% de los ciudadanos europeos (base de referencia: en diciembre de 2008 la cobertura DSL total era de un 93% de la población de la UE).
- **Banda ancha rápida para 2020**: cobertura de banda ancha de 30 Mbps o superior para el 100% de los ciudadanos europeos (base de referencia: en enero de 2010 un 23% de los abonos a la banda ancha alcanzaban al menos los 10 Mbps).
- **Banda ancha ultrarrápida para 2020**: un 50% de los hogares europeos deberán contar con abonos por encima de los 100 Mbps.

3.1.2 Mercado único digital

- **Promoción del comercio electrónico:** un 50% de la población deberá efectuar compras en línea para 2015. La base de referencia: en 2009, un 37% de usuarios con edades comprendidas entre los 16 y los 74 años habían efectuado pedidos de bienes o servicios con carácter privado en los 12 meses anteriores.
- **Comercio electrónico transfronterizo**: un 20% de la población deberá efectuar compras transfronterizas en línea para 2015. La base de referencia: en 2009, un 8%

de usuarios entre los 16 y los 74 años habían efectuado pedidos de bienes o servicios a proveedores de otros países de la UE en los 12 meses anteriores.

- **Comercio electrónico para las empresas**: un 33% de las Pymes deberán efectuar compras o ventas en línea para 2015. La base de referencia: en 2008, un 24% y un 12% de las empresas compró o vendió, respectivamente, de forma electrónica, por un valor igual o superior al 1% de su volumen total de compras o su facturación.
- **Mercado único de los servicios de telecomunicaciones:** para 2015 la diferencia entre las tarifas de itinerancia y las nacionales deberá aproximarse a cero. La base de referencia: en 2009, el precio medio de un minuto de itinerancia ascendía a 0,38 céntimos (por llamada efectuada), y el precio medio por minuto de todas las llamadas en la UE era de 0,13 céntimos (incluida la itinerancia).

3.1.3 Inclusión digital

- **Aumentar la utilización regular de Internet** de un 60% a un 75% en 2015 y, entre los colectivos desfavorecidos, de un 41% a un 60%. La base de referencia son las cifras de 2011.
- **Disminuir a la mitad la parte de población que nunca ha usado Internet para 2015** hasta un 15% La base de referencia: en 2009, un 30% de personas con edades comprendidas entre los 16 y los 74 años no había usado nunca Internet.

3.1.4 Servicios Públicos

- **Administración electrónica para 2015**: Un 50% de los ciudadanos utilizarán la administración electrónica, y más de la mitad de esa cifra cumplimentarán formularios en línea. La base de referencia: en 2009, un 38% de personas con edades comprendidas entre los 16 y los 74 años habían usado la administración electrónica en los 12 meses anteriores, y un 47% de ellas había cumplimentado formularios en línea.
- **Servicios públicos transfronterizos**: En 2015 deberán estar disponibles en línea todos los servicios públicos transfronterizos clave.

3.1.5 Investigación e innovación

- **Fomento de la I+D en las TIC**: Duplicación de la inversión pública a 11.000 millones de euros (base de referencia: la cifra nominal de créditos presupuestarios públicos de I+D dedicados a las TIC ascendía en 2007 a 5.700 millones).

3.2 SITUACIÓN GENERAL POR SERVICIO

3.2.1 Telefonía fija

La **telefonía fija** en la Unión Europea de los 27, **continuó el lento declive** que muestra desde hace años. En 2012, en la UE (27) se estima una **disminución de 10 millones de líneas fijas**, lo que supone una caída del 5,5%. Las previsiones indican que se mantendrá esta tendencia en los próximos años ya sea por la **sustitución del acceso fijo por el móvil** o por el **uso de aplicaciones que permiten realizar llamadas VoIP.** Además**,** el volumen de **ingresos** generados sí presentó una **reducción significativa del 9,0%**.

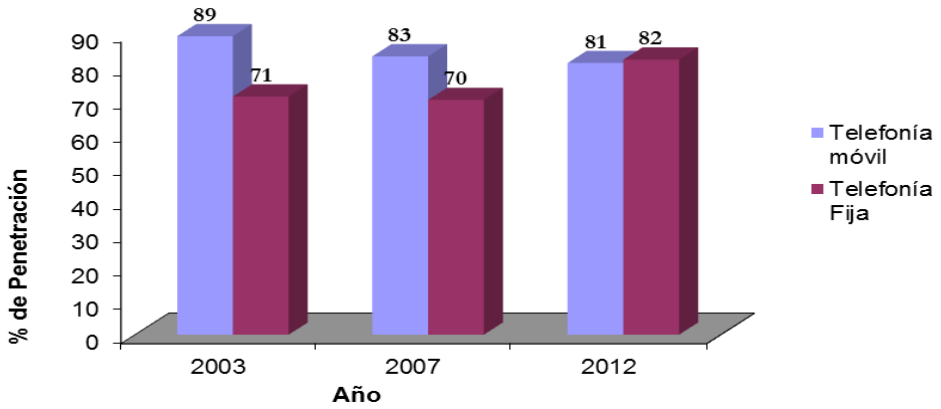


Gráfico 3.2.1 Penetración de la telefonía fija en los hogares de la UE. Elaboración propia Fuente: CMT 2012

3.2.2 Telefonía móvil

En Europa, la **penetración de la telefonía móvil es muy alta**, con **132 líneas por cada 100 habitantes**. Aun así, en 2012, el parque de altas de telefonía móvil aumentó un 2,4%. Los **ingresos globales de telefonía móvil cayeron el 0,5%** en el año debido a que los ingresos de voz cayeron el 5,8% ya que se produjo una **disminución de los precios de las**

llamadas de voz. Cabe destacar que España **es el segundo país de la UE con mayor cantidad de números portados en 2012**, sólo por detrás de Italia.

La **penetración de Internet móvil** de banda ancha, medida por el número de tarjetas de datos (datacards) y módem USB dedicados por cada 100 habitantes, **se sitúa en España ligeramente por encima de la media de la UE,** al contrario de lo que sucede con la tasa de penetración de las líneas móviles (Gráfico 4.2.2).

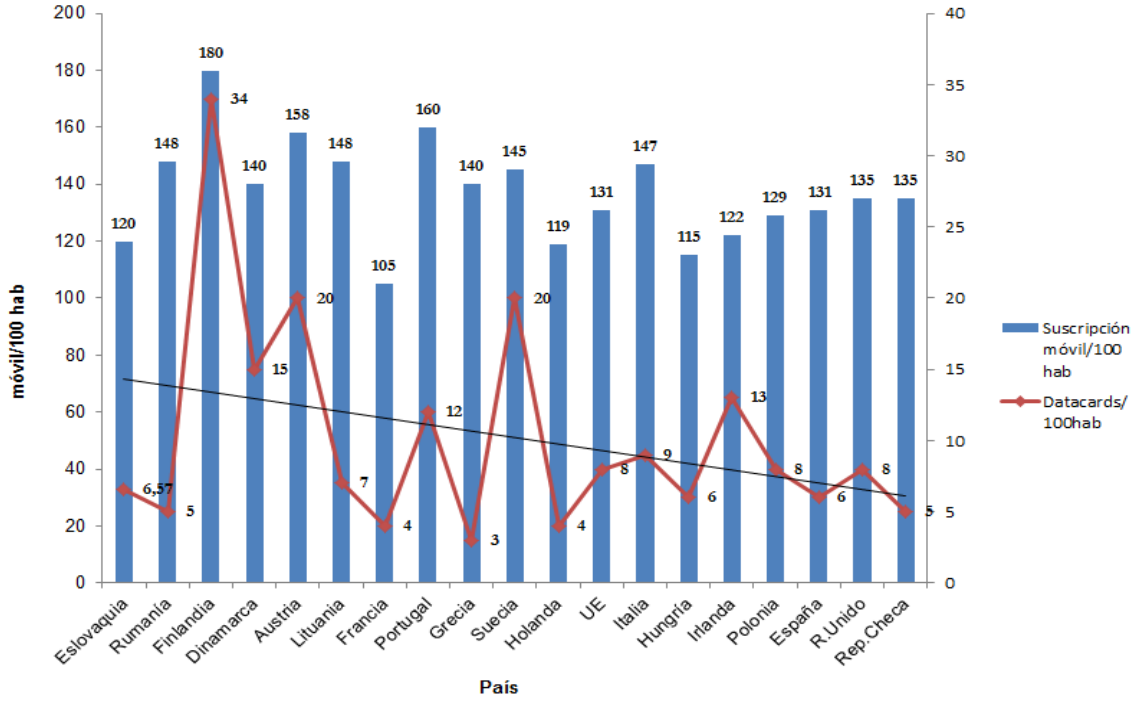


Gráfico 3.2.2 Tasa de penetración de la telefonía móvil y datacard en los hogares de la UE. Elaboración propia .Fuente: Informe e2012 de la Fundación Orange

La apuesta por Internet móvil y el tráfico de datos ha provocado que en **2012 España sea el segundo país de la UE con mayor penetración de terminales inteligentes**. Por cada 100 suscripciones españolas, 35 están asociadas a un smartphone, dato sólo superado por Suecia, donde la ratio es de 40 terminales inteligentes por cada 100 líneas (Gráfico 9.2.3).

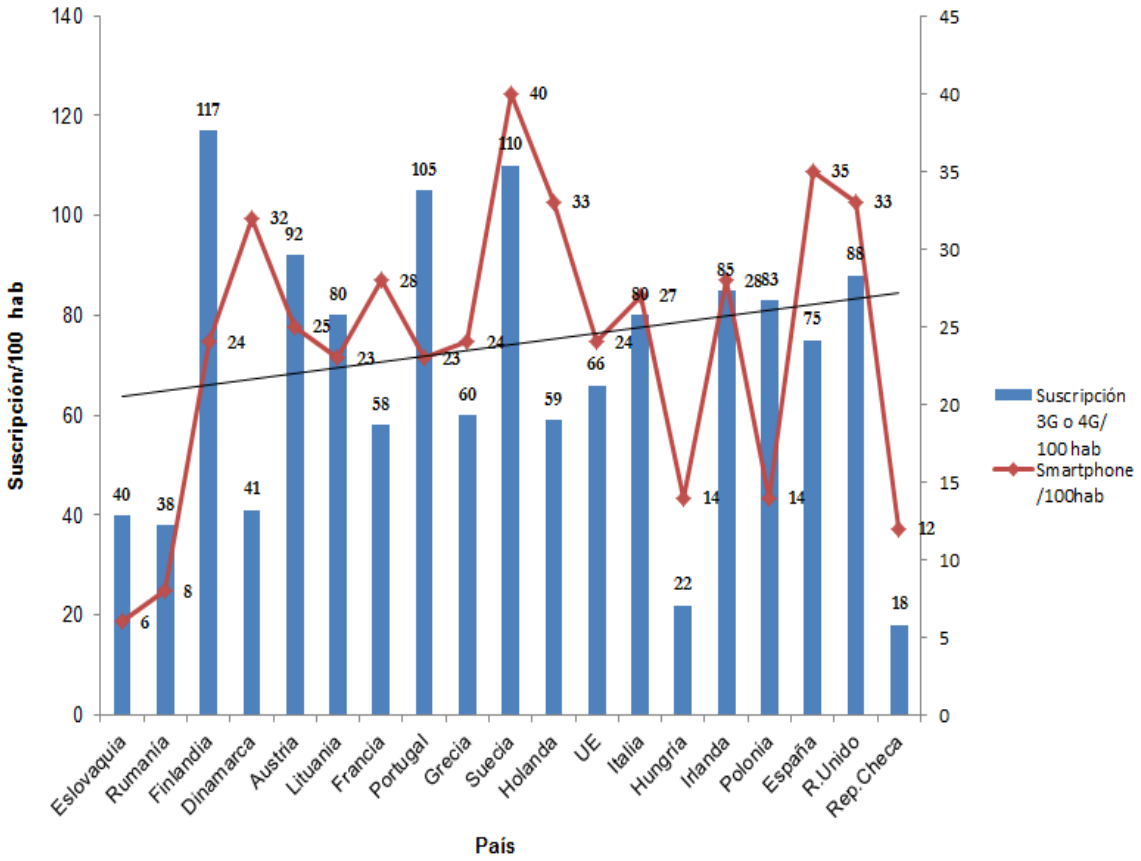


Gráfico 3.2.3 Tasa de penetración de smartphones y suscripciones 3G. Elaboración propia .Fuente: Informe e2012 de la Fundación Orange

Es probable que en el futuro el crecimiento se vea parcialmente truncado debido cambio de política de **operadores que han decidido dejar de subvencionar la adquisición de terminales inteligentes** en España.

3.2.3 Banda ancha Fija

La banda ancha fija **mantiene la tendencia creciente**, a pesar de la fuerte competencia en el sector y la crisis económica de nuestro entorno. Las conexiones de banda ancha por redes fijas **aumentaron en la UE el 5,4% en 2012**, lo mismo que la penetración, que alcanzó las 29 líneas por cada 100 habitantes, y se espera continúe aumentando a tasas del 4,9% anual de media en los próximos tres años.

3.2.3.1 Hogar

Las conexiones de **banda ancha en el hogar** experimentan una subida **de 6 puntos porcentuales respecto a 2011, hasta alcanzar un 67%** de media en la UE27 en 2012**.**

España con el 62% cuenta con un porcentaje ligeramente inferior al de la media comunitaria.

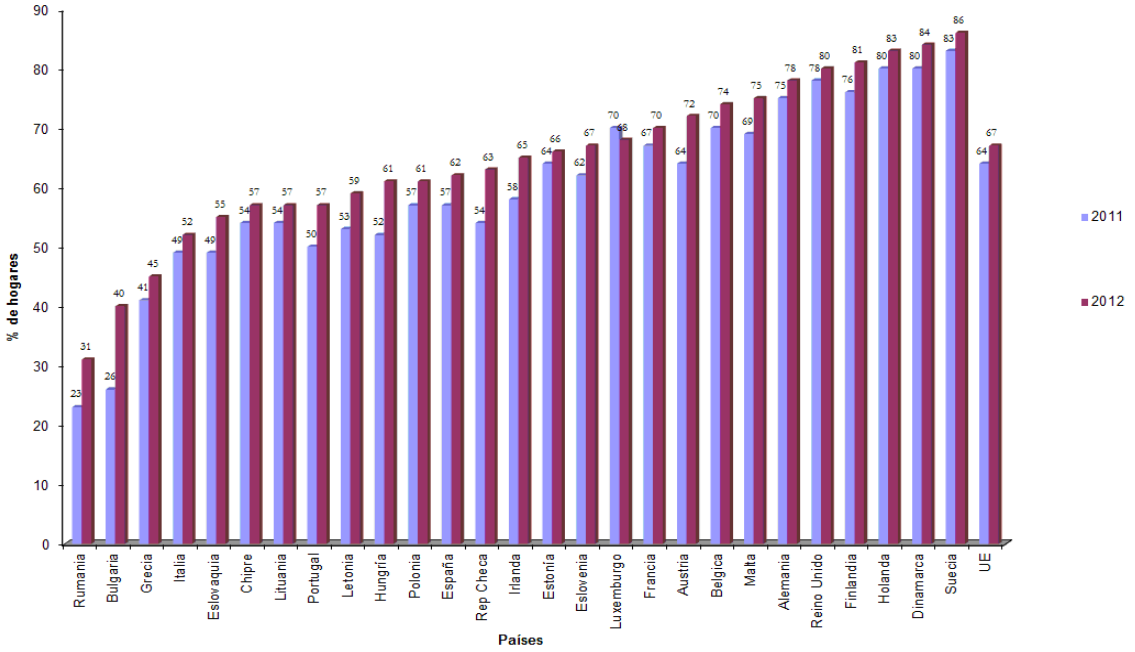


Gráfico 4.2.4 Hogares conectados a Internet a través de la banda ancha. Elaboración propia .Fuente: Informe Anual La Sociedad en Red 2012 del ONTSI

3.2.3.2 Empresas

En el ámbito de las **empresas la banda ancha está más extendida y en 2012 aproximadamente 9 de cada 10 empresas la utilizan como tecnología de conexión a Internet.** España mantiene su posición entre el conjunto de países líderes con un 96%. Cabe destacar que más de la mitad de los miembros de la Unión cuentan con porcentajes **de empresas con banda ancha del 90%** o más.

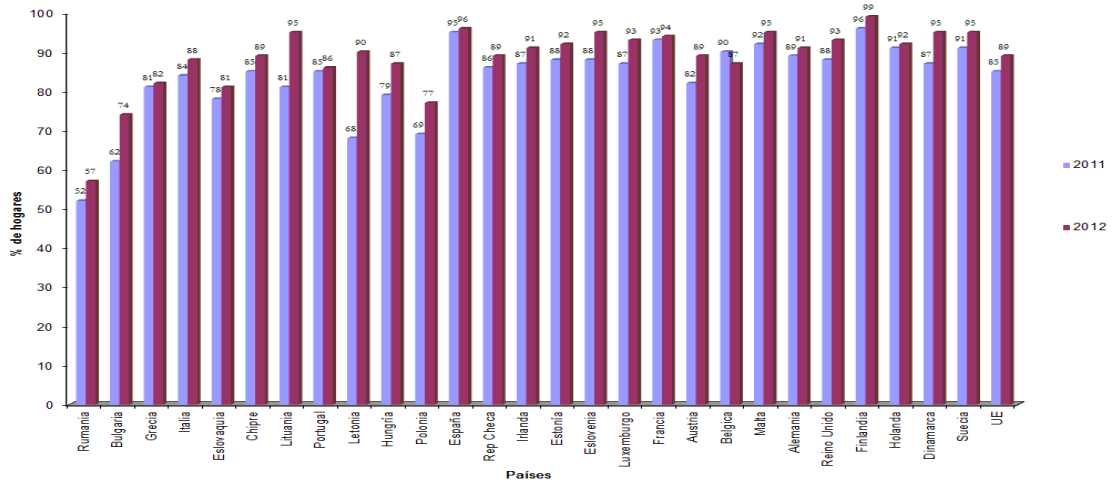


Gráfico 3.2.5 Empresas conectados a Internet a través de la banda ancha. Elaboración propia .Fuente: Informe Anual La Sociedad en Red 2012 del ONTSI

3.2.3.3 Tecnología

Por tecnología, el **acceso a través de xDSL** sigue siendo el **más popular al contar con el 78%** de las líneas, aunque crece con popularidad la **posibilidad de conectarse a través de WiFi o FTTH** (fibra al hogar). Sin embargo, estas modalidades siguen siendo escasas en España, con **una penetración** sobre el total de conexiones de banda ancha de un **0,7% para WiFi y un 1,5% para FTTH**.El acceso **WiFi-WiMax es la principal vía de acceso a Internet de banda ancha en áreas rurales**. **En el despliegue de la fibra óptica, España se está quedando atrás respecto a otros países, ya que la media europea se sitúa en el 1,8%.**

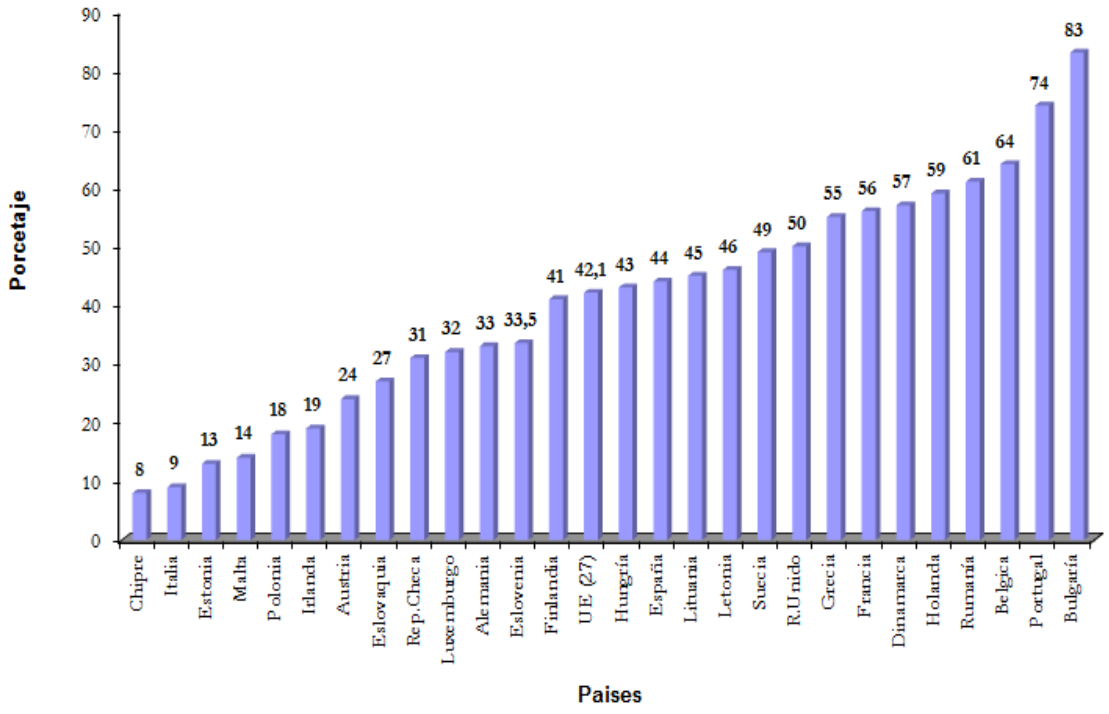


Gráfico 3.2.6 Tasa de penetración de banda ancha fija de alta velocidad por cada 100 hab. Elaboración propia .Fuente: Informe CMT 2011

Destacar que **España tiene uno de los mayores costes de acceso en Europa**, junto con Malta, Irlanda y Chipre, donde los precios se justifican por la **alta cuota en el mercado mayorista del operador dominante**, lo que hace que se frene la competencia.

3.2.4 Banda ancha Móvil

El **crecimiento más alto** se dio en el **uso de Internet mediante las redes para comunicaciones móviles**. En la UE(27) la cobertura media de las redes 3G-UMTS alcanzó en 2012 al 94% de la población. Esta cobertura tan amplia y las inversiones realizadas en el despliegue de las redes 4G han hecho posible satisfacer la demanda creciente y en el periodo 2009-2012 la **penetración de tarjetas de datos (datacards) se ha multiplicado por dos** en la UE(27), y también en España, y se ha alcanzado una penetración **de 7,6 líneas datacards** por cada 100 habitantes.

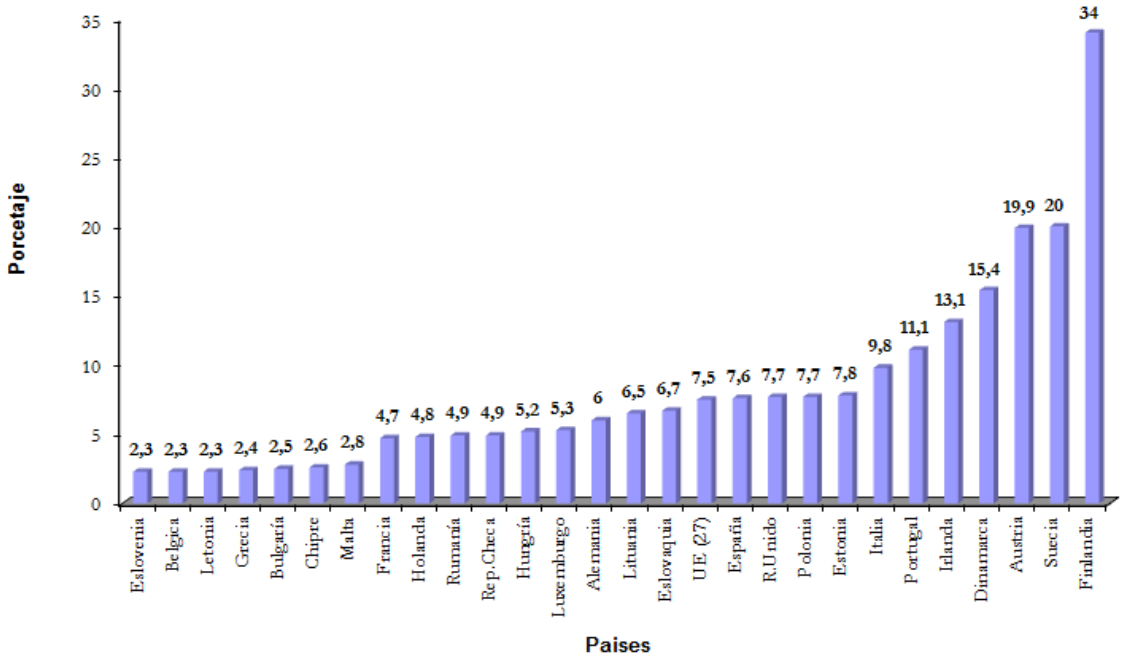


Gráfico 3.2.7 Penetración de banda ancha móvil con datacards por cada 100 hab. Elaboración propia .Fuente: Informe CMT 2012

3.2.5 Internet

En **2012 un 68% de los ciudadanos europeos utiliza Internet de manera habitual**, es decir, al menos una vez a la semana. Representa un crecimiento de 3 puntos respecto al 2011. En Suecia y Holanda, líderes comunitarios, 9 de cada 10 individuos son usuarios regulares de la Red. **España, por su parte, se encuentra 6 puntos por debajo, habiendo experimentado una subida de 4 puntos en el último año**.

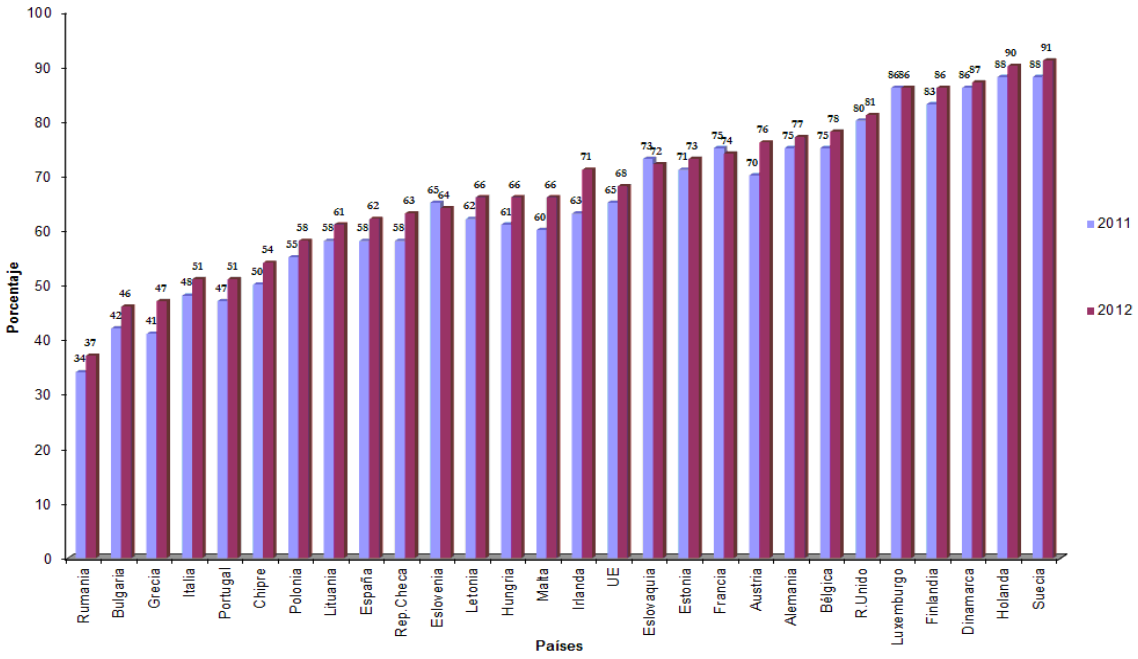


Gráfico 3.2.8 Porcentaje de uso de Internet en la UE por parte de los ciudadanos. Elaboración propia .Fuente: Informe Anual La Sociedad en Red 2012 del ONTSI

3.2.5.1 Usos de Internet

La **búsqueda de información sobre bienes y servicios** (con más de la mitad de la población) y **la lectura de periódicos y revistas en línea** (40%) destacan como los dos **usos principales de Internet** por parte de los internautas europeos en el año 2012. Un patrón similar se observa en España a los europeos.

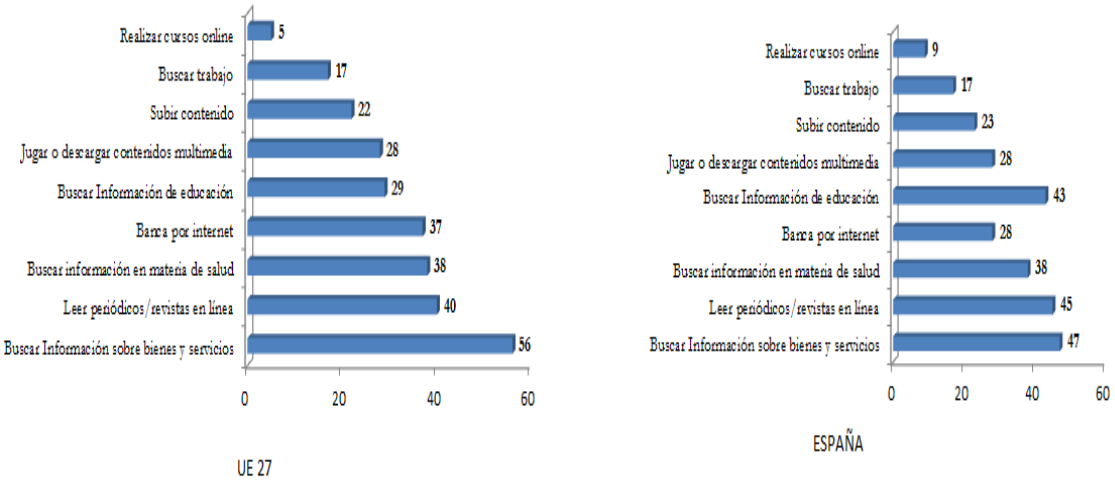


Gráfico 3.2.9 Principales usos de Internet en la UE y España por parte de los ciudadanos. Elaboración propia .Fuente: Informe Anual La Sociedad en Red 2012 del ONTSI

3.3 SITUACIÓN EN MATERIA ECONÓMICA

En 2012, el **sector de telecomunicaciones redujo su facturación en la UE (27) en un 1,9%.** La zona euro registró un **crecimiento negativo del 0,5%. Se estima que el sector crezca a tasas inferiores a las del PIB** al igual que en los últimos años. En un contexto de salida muy lenta de la **crisis económica**, y con algunos países en recesión, los **operadores de telecomunicaciones reaccionaron disminuyendo los precios**. El índice general de precios (IPC) de la economía española creció el 2,4% según el informe de la CMT y el **subíndice de precios de comunicaciones disminuyó un 3,3%, la mayor caída registrada en una década**. Este descenso fue mayor en comparación que el de en la UE(27) para este conjunto de servicios, que fue del 1,6%.

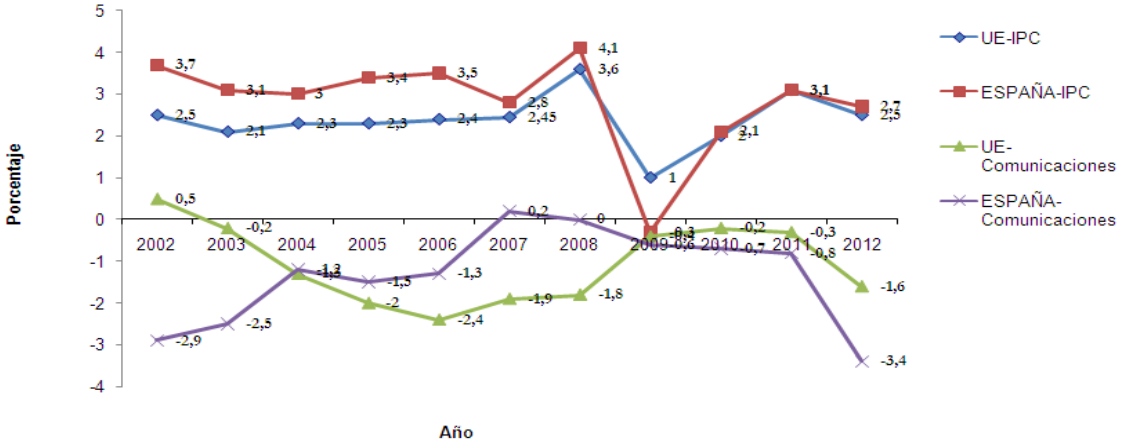


Gráfico 3.3.1 Tasa de variación del IPC y del índice de comunicaciones en la UE y España. Elaboración propia .Fuente: Informe CMT 2011

3.3.1 Gasto en TI

El gasto en TI representó **en 2012 un 2,6% del PIB en la UE**, mientras que el correspondiente a **Comunicaciones ascendió al 2,8%. La posición de España en este ranking es similar a la de años anteriores, con porcentajes de gasto por debajo de la media europea**, aunque se detecta un cierto ascenso del gasto en TI y un ligero descenso en el de Comunicaciones, donde se sigue superando la media europea.

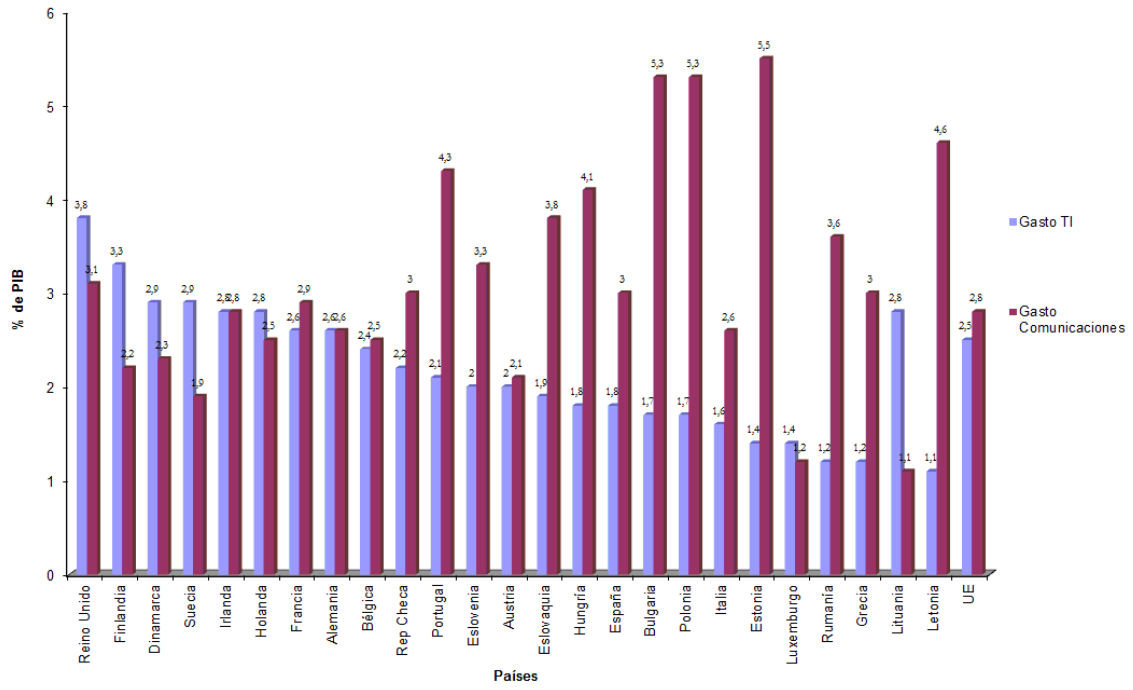


Gráfico 3.3.2 Gasto en TIC y Comunicaciones expresado con % del PIB. Elaboración propia .Fuente: Informe e2012 de la Fundación Orange

4.3.2 Inversión en TI

Respecto al TIC a **pesar de su escaso peso en términos de contribución al PIB**, el **5,71% del total de la inversión bruta en bienes tangibles en España proviene de estos sectores TIC,** porcentaje cercano al de países con mayor desarrollo económico como Alemania y superior al de Suecia o Noruega.

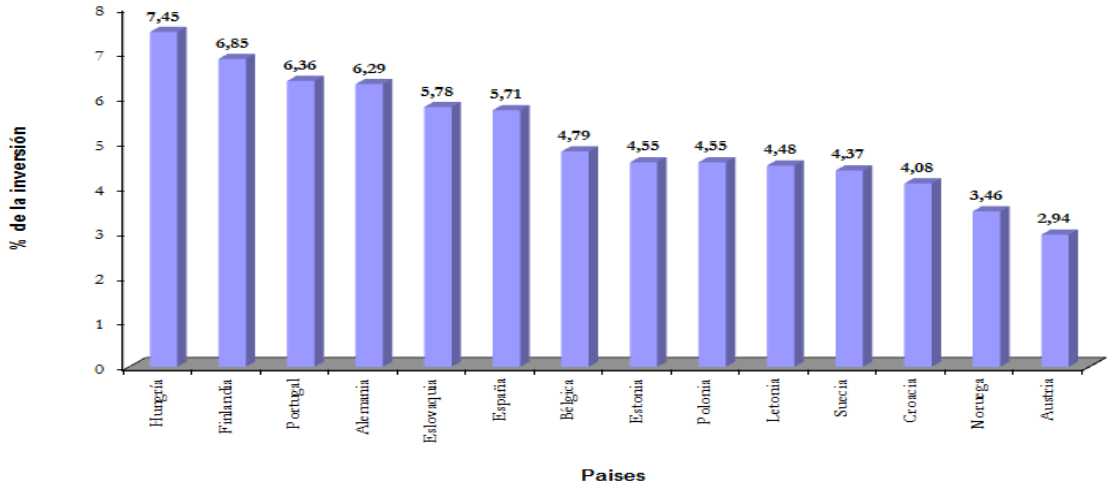


Gráfico 3.3.3 Inversión bruta en el sector TIC como porcentaje de la inversión total. Elaboración propia .Fuente: Informe e2012 de la Fundación Orange

4. SECTOR DE LAS TELECOMUNICACIONES EN ESPAÑA

En el análisis se estudia cómo está el mercado global de las telecomunicaciones en España y las tendencias de uso que se está realizado sobre los servicios y equipamientos de telecomunicaciones.Las **dificultades de la situación de la economía española** de los últimos años tuvieron también **repercusión en el sector de las telecomunicaciones**. El mercado se encuentra en disminución durante estos últimos años, ya que desde 2008 acumula una **reducción de ingresos del 13%**. La fuerte **competencia en precios** o la **sustitución de tráfico de voz y mensajes cortos** por tráfico de datos puede explicar dicha **caída de ingresos**.

Los **operadores debido al descenso del consumo** optaron por **rebajar sus precios, aumentando las promociones de sus servicios** o añadiendo servicios adicionales con descuentos a los paquetes ya existentes en integración de servicios de hasta 4 y 5 plays. Las **reducciones de los precios** impactaron negativamente en los ingresos de la mayoría de los servicios finales, pero no **disminuyeron ni la penetración ni los consumos de los usuarios**. A lo largo de 2012, tanto la penetración de la **banda ancha, como la de la televisión de pago y la del servicio telefónico móvil aumentaron**. Muy notable fue el incremento de la penetración de la banda ancha a través de redes para comunicaciones móviles, en especial mediante smartphones, tabletas y otros dispositivos.

4.1 MERCADO GLOBAL DE LAS TELECOMUNICACIONES EN ESPAÑA

4.1.1 Materia Económica

4.1.1.1 Ingresos

Dada la situación de crisis que vivimos en la actualidad, el mercado de las telecomunicaciones no iba a librarse de ella y los **ingresos por servicios finales disminuyeron un 7,4% debido a la bajada del consumo y de los precios de los servicios**. En 2012 la cifra total del sector descendió un 7,2% respecto del año anterior. Continuó por tanto la tendencia a la baja de los ingresos iniciada en 2009. **El único servicio que creció fue el de banda ancha móvil, con un aumento del 29%.**

	2011	2012	VARIACIÓN 12/11
Comunicaciones Fija	10786.09	10021.43	-7.1%
Telefonía Fija	5387.91	488.86	-10.7%
Banda Ancha Fija	3833.76	3659.01	-4.6%
Com. Empresa	1501.37	1497.28	-0.3%
Info. Telefónica	63.06	51.29	-18.7%
Comunicaciones Móviles	13450.13	12271.10	-8.8%
Telefonía Móvil	11305.23	9504.46	-15.9%
Banda Ancha Móvil	2144.90	2766.64	29%
Serv. Audiovisuales	4125.03	3761.43	-8.8%
Resto	3178.93	3166.38	-0.4%
Total	31540.18	29220.34	-7.4%

Tabla 4.1.1 Ingresos por servicios finales 11/12 (millones de euros). Elaboración propia .Fuente: Informe CMT 2012

Los servicios de banda ancha fija y móvil aumentaron su participación al total de ingresos finales y llegaron a representar el 22% de estos, frente al 19% de 2011.Pero los **servicios de telefonía móviles en conjunto perdieron peso en el sector** debido al **descenso en los servicios de voz y de mensajes por culpa de la mensajería instantánea como Whatsapp o Line** a pesar de los esfuerzos de los operadores en regalar los SMS o bajar el precio de estos.

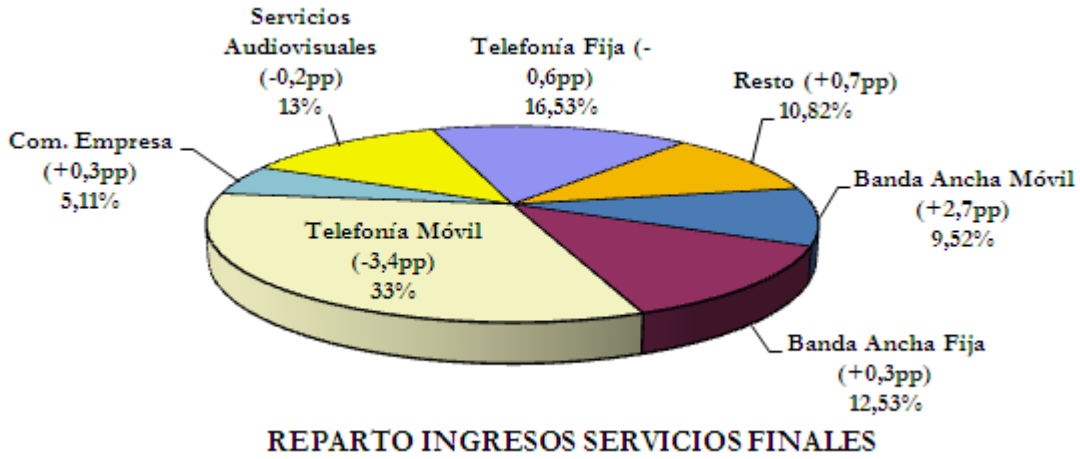


Gráfico 4.1.1 Porcentaje de la distribución de ingresos de los servicios finales.Elaboración propia .Fuente: Informe CMT 2012

Los servicios mayoristas disminuyeron también su facturación un 6,3%, debido sobre todo a la bajada en los precios de los servicios de interconexión más demandados en redes fijas y móviles.

	2011	2012	VARIACIÓN 12/11
Interconexión	4114.20	3698.86	-10.1%
Alquiler de Circuitos	741.29	747.75	0.9%
Tx de datos	41.98	51.37	22.4%
Servicio ADSL	545.57	593.29	8.7%
Transporte y difusión	413.51	394.50	-4.6%
Otros Servicios	553.78	522.19	-5.7%
Total	6410.33	6007.96	**-6.3%**

Tabla 4.1.2 Ingresos por servicios mayoristas 11/12 (millones de euros). Elaboración propia .Fuente: Informe CMT 2012. Elaboración propia

4.1.1.2 Inversión

Los operadores invirtieron más de 4.000 millones de euros en 2012. **La reducción fue del 8,9% respecto a lo invertido en 2011** si no se incluyen los desembolsos de los operadores por los pagos (1500 millones) de la asignación del espectro radioeléctrico realizado en 2011.

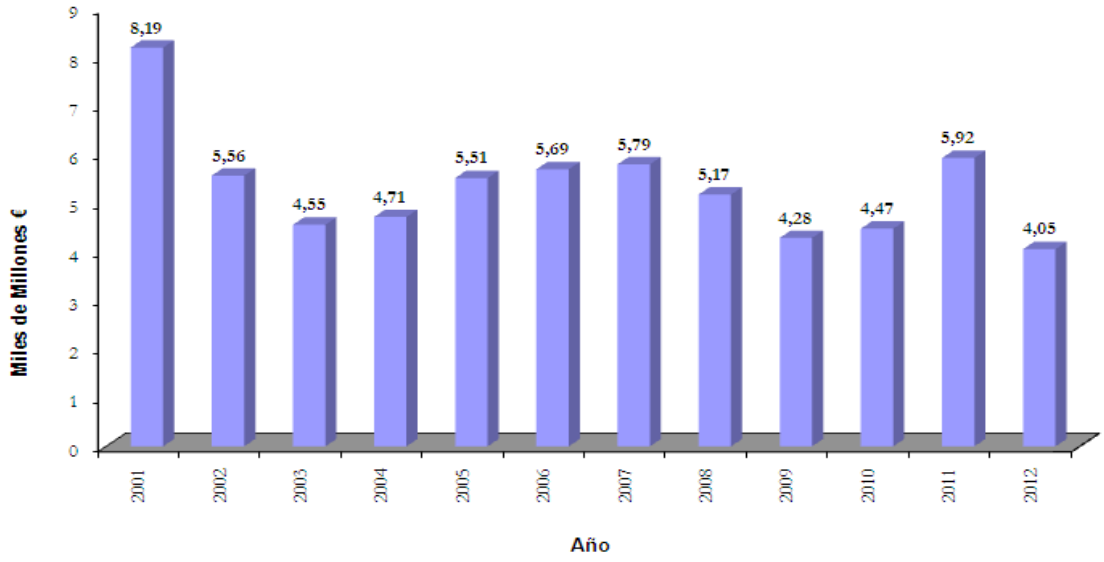


Gráfico 4.1.2 Inversión realizada por los operadores en miles de millones de €. Fuente: Informe CMT 2012. Elaboración propia

La **inversión fue realizada**, en gran parte, por la **extensión de la cobertura** de las redes móviles que ha conseguido que el 95% de la población pueda acceder, al menos, a una red **3G/UMTS y el comienzo de las redes 4G/LTE** en las principales capitales de provincia. En el ámbito de las redes fijas, continuó el proceso de **transformación de la red de cobre hacia una red de fibra óptica** por parte de los operadores conocidas como redes de nueva generación (NGA), Además, continúa el proceso de actualización tecnológica que supone la implantación del DOCSIS 3.0 en las redes de cable híbridas de fibra y coaxial (HFC) .En cuanto a los datos por operador, los principales operadores, excepto Telefónica y Movistar, aumentaron su inversión en 2012.

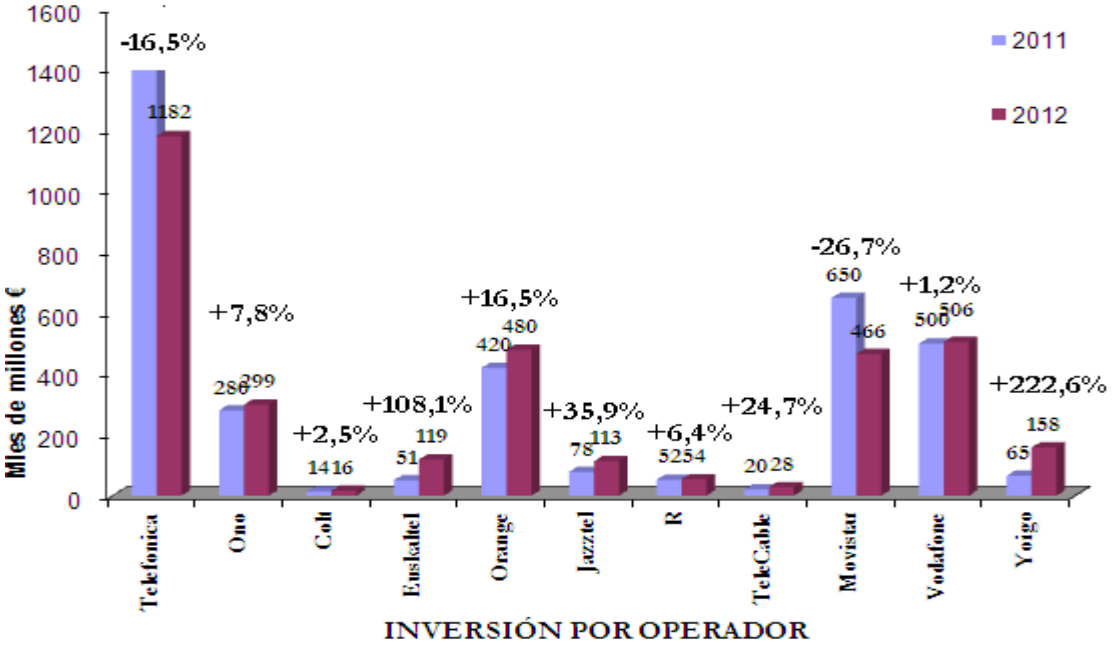


Gráfico 4.1.3 Inversión realizada por cada operador en los años 2011 y 2012 en miles de millones de €. Fuente: Informe CMT 2012. Elaboración propia

4.1.2 Situación de los servicios finales

4.1.2.1 Penetración

A pesar de la situación de crisis económica, los datos de penetración de los distintos servicios de telecomunicaciones vienen mostrando, en general, un **aumento en lo que se refiere a la banda ancha, tanto fija como móvil**. Así, en 2012, la penetración de la **banda ancha fija aumento ligeramente, en 0,7 puntos** porcentuales respecto a 2011.

Por el contrario, **la banda ancha móvil creció significativamente hasta alcanzar las 54 líneas por cada 100 habitantes** (datacards y smartphones), 16,5 puntos porcentuales más que al año anterior. Este crecimiento vino dado por el más que significativo aumento de conexiones a redes 3G/UMTS a través de terminales smartphone y a la demanda de estos últimos dispositivos. Las penetraciones del resto de servicios disminuyeron al igual que en años anteriores. Destacar que el **total de líneas móviles disminuyó un 3,7%,** debido a una reducción significativa de las líneas prepago (más de 2 millones).

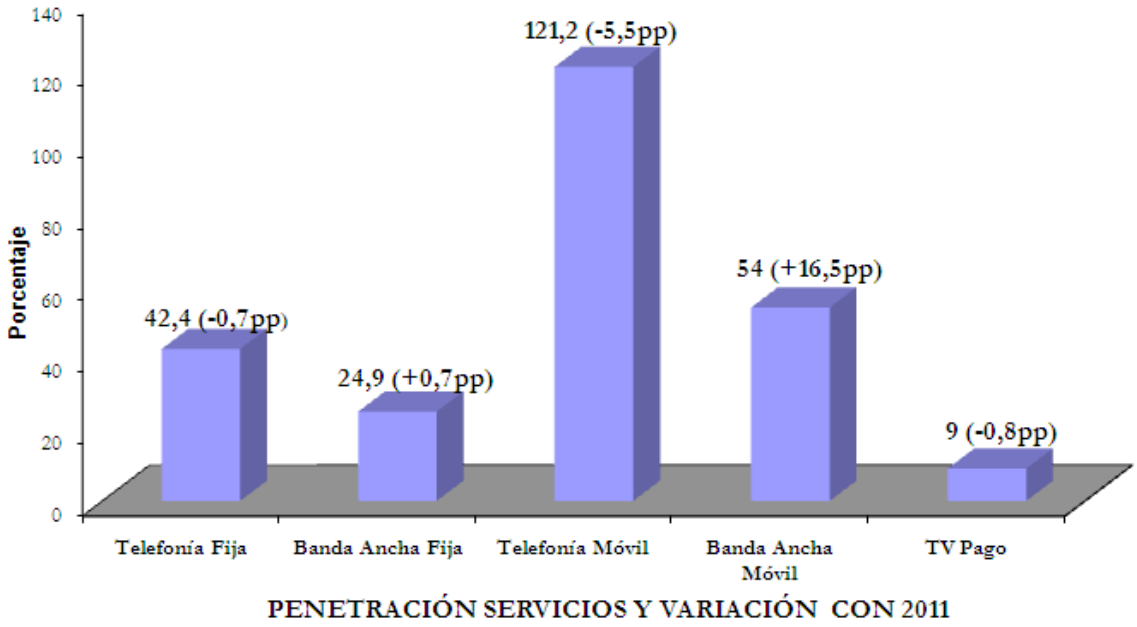


Gráfico 4.1.4 Porcentaje de penetración de servicios y variación de puntos porcentuales con 2011. Fuente: Informe CMT 2012. Elaboración propia

4.1.2.2 Integración o empaquetado de los servicios

El año 2012 supuso un cambio importante en el empaquetamiento de servicios ya que **aparecieron los paquetes cuádruple y quíntuple, que integran los servicios de comunicaciones fijas y móviles.** Los niveles de contratación de este tipo de paquetes (cuádruples y quíntuples) tuvo una gran demanda y buena acogida por los clientes de Telefónica y de los operadores alternativos de xDSL.

Para recuperar cliente perdidos y cuota de mercado, **en octubre de 2012, Telefónica lanzó Movistar Fusión, que comercializaba por vez primera en una única oferta los servicios de voz y banda ancha tanto fija como móvil**, además de la televisión de pago

en el caso del quíntuple play. Otros operadores también lanzando ofertas similares de cuádruple play a lo largo del último trimestre del año. **Este empaquetamiento de los servicios supusieron una importante rebaja de los precios de los servicios** lo que implico que a finales de 2012, ya había más de un millón de paquetes con cuatro servicios (voz fija y móvil más banda ancha fija y móvil). A estos paquetes cuádruples se les sumaron 146.132 paquetes quíntuples, que incorporan la televisión de pago a los cuatro servicios anteriores. Cada vez hay menos líneas sin empaquetar para los distintos servicios. **Este tipo de empaquetamiento de los servicios hizo que los clientes se acogiese a estas ofertan manteniendo su operador actual y no portando los servicios a la competencia.**

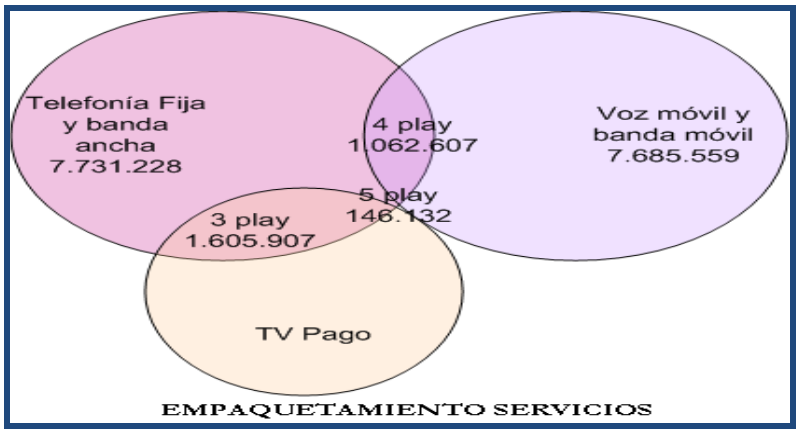


Gráfico 4.1.5 Empaquetamiento de los servicios en número de unidades. Fuente: Informe CMT 2012. Elaboración propia

El servicio de banda ancha fija ofrecido junto con el servicio de telefonía fija alcanzó un porcentaje del 69,2%. Además, los paquetes (cuádruple play) que también incluyen el servicio de banda ancha móvil y el de voz móvil alcanzaron el 9,4%. **Los paquetes de triple play supusieron el 16,6% de las líneas, por tanto, la tendencia es unir las comunicaciones móviles y fijas en una misma facturación para ahorrar costes.**

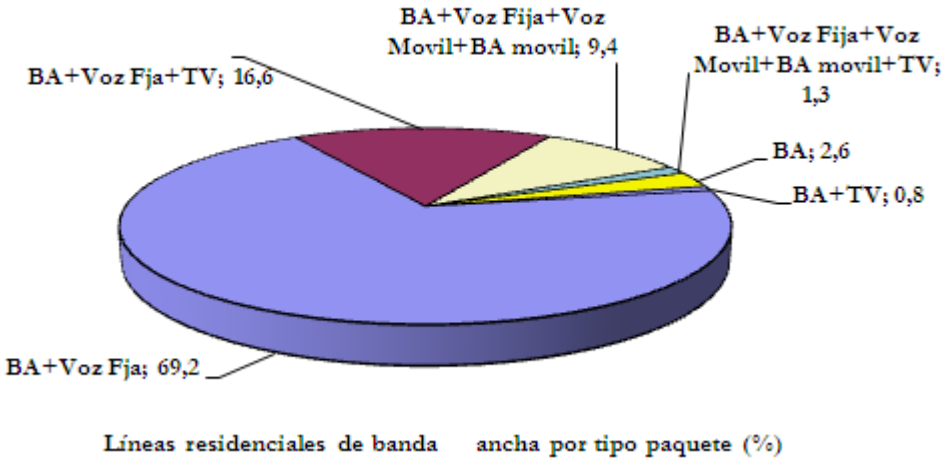


Gráfico 4.1.6 Porcentaje de líneas residenciales de banda ancha empaquetadas. Fuente: Informe CMT 2012. Elaboración propia

4.1.2.3 Precio y gasto en la contratación de los servicios

Los operadores reaccionaron a la crisis económica y al bajo consumo reduciendo sus tarifas y empaquetando sus servicios. Así, **el gasto medio** de un hogar por la banda **ancha fija y voz fija se redujo un 6,9%.** En el caso del paquete triple, la reducción fue del 5,1%.En el segundo y tercer trimestre de 2012, el gasto total de los hogares que contrataban servicios de telefonía fija, telefonía móvil, banda ancha fija y banda ancha móvil se situaba sobre los 92 euros por mes. En cambio, a finales de año, y como resultado de los servicios empaquetados, el gasto se redujo hasta los 84,9 euros mensuales.

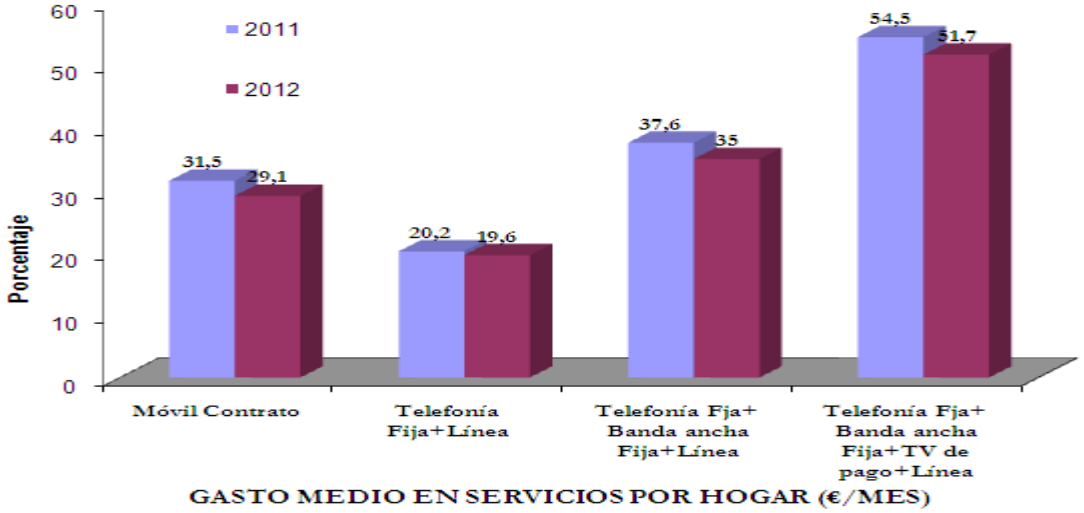


Gráfico 4.1.7 Porcentaje de gasto medio en servicios por hogar. Fuente: Informe CMT 2012. Elaboración propia

4.1.2.4 Infraestructuras y tecnologías

Si analizamos la evolución de las líneas en función de la tecnología antes habría que agruparlas:

1) Para ello tendríamos las soportadas sobre **redes fijas**: como son las tecnologías xDSL sobre el par de cobre; las tecnologías sobre redes de cable, como las redes HFC mediante un soporte mixto de fibra óptica y cable coaxial; y, finalmente, las tecnologías sobre redes de fibra óptica, como por ejemplo los accesos FTTH.

2) Las tecnologías sobre **redes inalámbricas**: LMDS, Wi- MAX (cobertura de grandes distancias) y Wifi (entorno de cobertura reducido).

3) Las redes soportadas por **sistemas de satélite** como los VSAT.

4.1.2.4.1 Infraestructuras en redes fijas

En 2012, continuó la actualización y mejora de las redes fijas para permitir un mayor ancho de banda y más calidad de servicio. Respecto a las redes NGA, **continuó el notable avance en el despliegue de accesos FTTH por parte de Telefónica**. Asimismo, otros operadores también llevaron a cabo despliegues de fibra óptica. **A finales de 2012, se llegó a los 3,25 millones de accesos FTTH instalados, el doble que los del año anterior con una cuota del 10,9%.** En cuanto a los **accesos HFC** se continuaron instalando nuevos accesos y mejorando su capacidad **hasta alcanzar los 9,8 millones de líneas** y una **porción de mercado del 33%. Mencionar que el par de cobre con tecnología xDSL es el que sigue teniendo mayor cuota de mercado en la actualidad.**

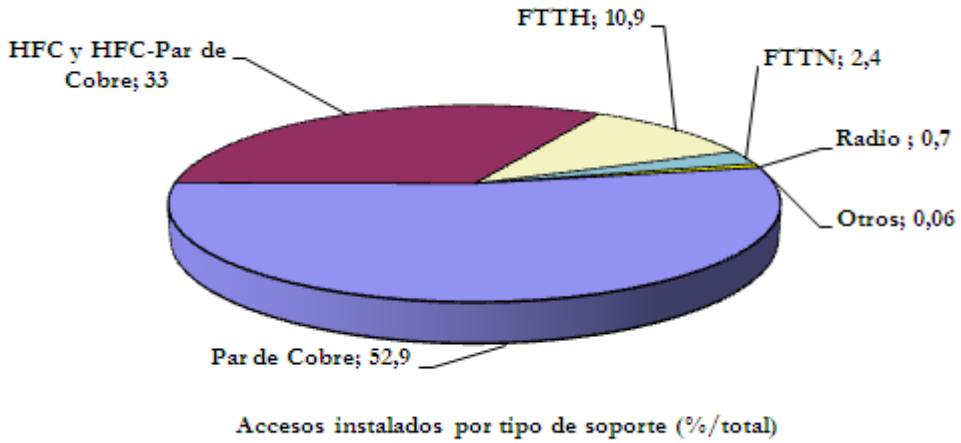


Gráfico 4.1.8 Porcentaje de accesos instalados por tipo de soporte. Fuente: Informe CMT 2012. Elaboración propia

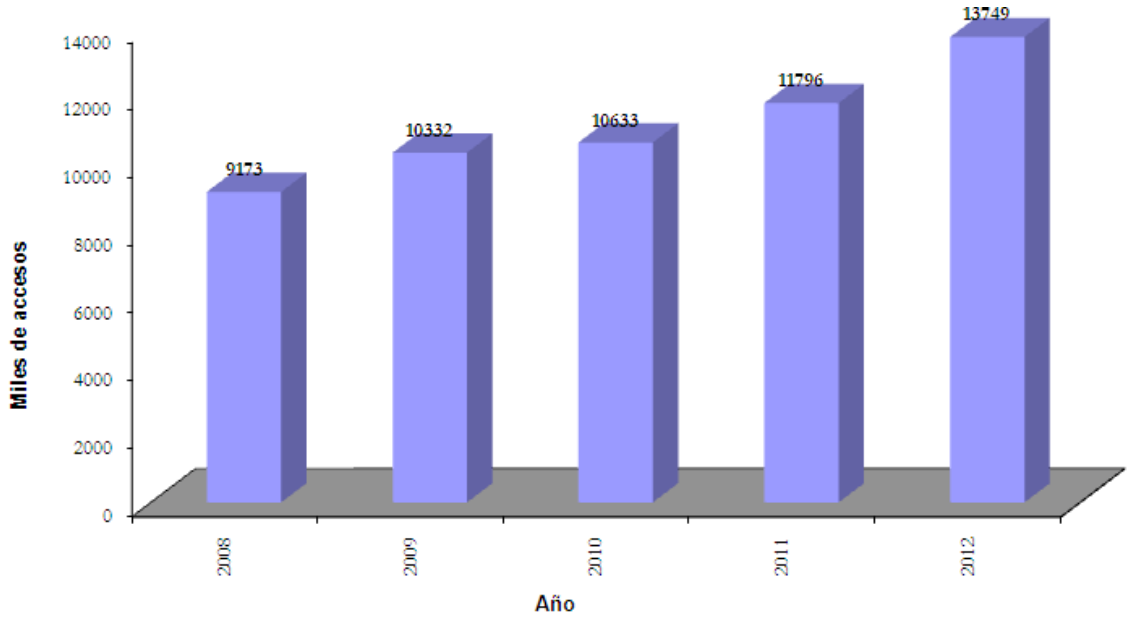


Gráfico 4.1.9 Evolución de los accesos instalados de HFC, HFC-Par Cobre y fibra. Elaboración propia. Fuente: Informe CMT 2012. Elaboración propia

En cuanto a la evolución de la velocidad, **con el despliegue del la fibra (FTTH) y la actualización de los nodos a DOCSIS 3.0 ha permitido la contratación de líneas de mayor ancho de banda**. Asimismo, a pesar de las limitaciones de la red de cobre, los operadores alternativos de xDSL también lanzaron ofertas de mayores velocidades de conexión (hasta 30 Mbps) mediante la tecnología VDSL En concreto, a finales de año, el 63% de las líneas de banda ancha contratadas contaba con una velocidad de conexión de 10

Mbps o superior, frente al 54% del año anterior. Además, el 10,5% de las líneas tenía una velocidad de conexión superior a los 20 Mbps.

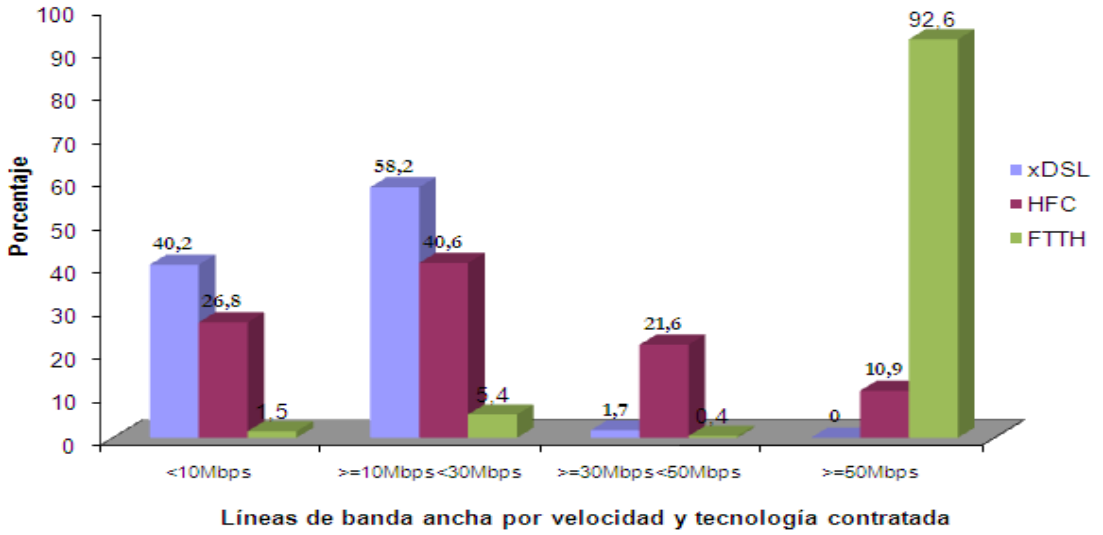


Gráfico 4.1.10 Porcentaje de líneas de banda ancha en función de la velocidad y la tecnología. Fuente: Informe CMT 2012. Elaboración propia

4.1.2.4.2 Infraestructuras en redes móviles

En el 2012 los operadores han realizado un **esfuerzo inversor y de despliegue para que la tecnología 3G prácticamente cubra todo el territorio nacional**, para ello las estaciones bases 3G aumentaron un 28,3% respecto al año anterior. **Por tanto, en el 2012 el 97,9% de la población ya está cubierta por una red 3G, ya sea UMTS o HSDPA.**

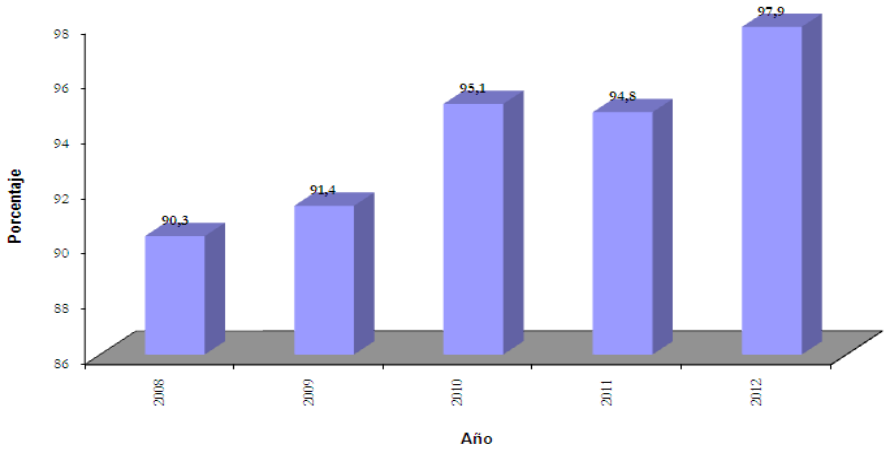


Gráfico 4.1.11 Porcentaje de la población cubierta por al menos una red 3G. Fuente: Informe CMT 2012. Elaboración propia

4.1.2.4.2.1 Cuarta generación móvil (4G)

Respecto a la **cuarta generación móvil (4G)**, el pasado julio de 2011, se concedieron las licencias del espectro quedando Vodafone con 60 MHz (2x30 MHz), Orange y MoviStar con la banda de 800Mhz. **La tecnología LTE (Long Term Evolution) permitirá velocidades de 100Mbps** y se encuentra en inicios de implantación en España. **Para más información de la tecnología LTE consultar el documento memoria_anex.pdf apartado ANEXO2.**

Debido al requerimiento de aumentos de ancho de banda surge la necesidad de hacer una **restructuración** de la arquitectura en las telecomunicaciones actuales. De hecho se ha convertido en una tendencia creciente en el mercado, ya que operadores como Orange, Vodafone, Yoigo y Movistar ya han estado lanzando al público sus redes LTE en respuesta a la saturación de las líneas actuales, lo cual representaría un desahogo importante para las ya fatigadas antenas 3G que en poco menos de 2 años han sido llenadas a poco más de su capacidad ideal, por lo que muchos usuarios han sentido una ineficiencia de la red a poco tiempo de haber entrado o después de llevar un prolongado tiempo con el servicio.

Primeramente esto se podría deber a la gran cantidad de planes libres disponibles con cada compañía que poco a poco van reduciendo sus precios en busca de más clientes, con lo que se crea un círculo vicioso indiscutible, más clientes para mejor red-mejor red para más clientes algo que se ve truncado debido a que los usuarios dejan de confiar en una red debido a su inestabilidad a causa de la saturación.

En lo referente a la implantación de las redes 4G/LTE ya se ha comenzado a comercializar en las principales capitales de provincia por todos los operadores principales. Destacar que mientras los operadores están implantando su propia red 3G, Telefónica, está llevando a cabo otro tipo de estrategia. Y es que, **mientras está desplegando sus propias redes, está usando la infraestructura de Yoigo**, como moneda de pago de prestar al operador su banda ancha. Con su propia red 4G, Telefónica prevé cubrir 63 municipios en 19 provincias para dar cobertura a casi la mitad de la población española. Para 2014 Orange asegura que cubrirá de cobertura 4G todas las capitales de provincia y Yoigo espera tener cubierto un 75% de la población.

4.1.2.5 Cuotas de mercado de los operadores

En este apartado se analizara que porción de mercado tiene los operadores de telecomunicaciones en función del servicio prestado.

4.1.2.5.1 Telefonía Fija

Respecto al servicio final de telefonía fija, **Telefónica continuo siendo el líder en cuanto a número de clientes se refiere pero continúo con un descenso de cuota** como en los últimos años. Este operador obtuvo el 58,4% de los clientes de acceso directo. Los operadores de cable captaron el 16,9% del total de clientes de acceso directo, mayoritariamente en el segmento residencial. Los demás operadores alternativos obtuvieron el 24,7%, lo que significó aumentar más de dos puntos porcentuales interanualmente. En ese grupo destacaron Jazztel y Vodafone. **Con el 12,4%, Ono fue el segundo operador por cuota de mercado.**

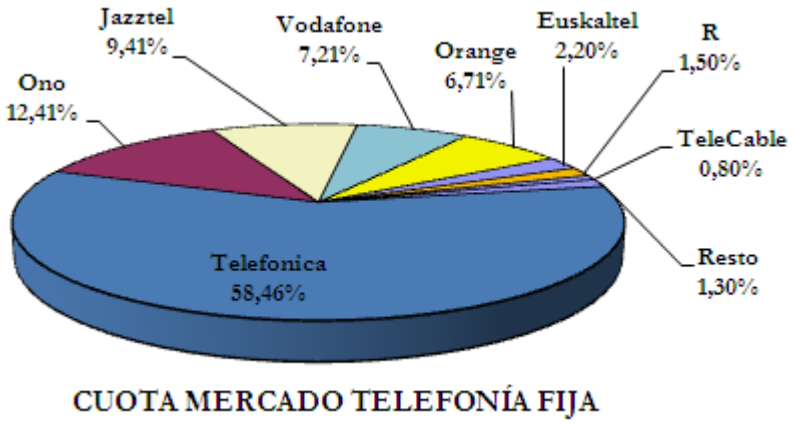


Gráfico 4.1.12 Porcentaje de cuota de mercado de los operadores en telefonía fija. Fuente: Informe CMT 2012. Elaboración propia

4.1.2.5.2 Telefonía Móvil

En el año 2012, los dos principales operadores **(Vodafone y Movistar) redujeron su cuota de mercado por número de líneas de voz móvil** ya que el resto de operadores (Orange, Yoigo y los OMV) vieron aumentadas las suyas. **Yoigo y los OMV fueron los que mayor participación ganaron en el año** y alcanzaron una cuota de mercado conjunta del 16%.

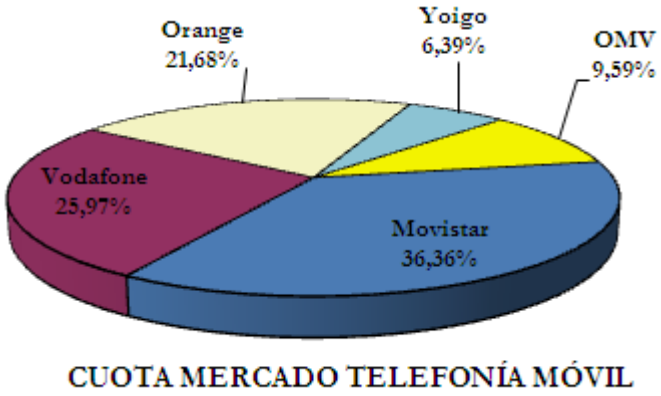


Gráfico 5.1.13 Porcentaje de cuota de mercado de los operadores en telefonía móvil. Fuente: Informe CMT 2012. Elaboración propia

4.1.2.5.3 Banda Ancha Fija

Telefónica siguió líder en el mercado empresarial, en el que su cuota aumentó medio punto hasta alcanzar el 74,9% con respecto al año pasado. El resto de los operadores tuvieron poca cuota de mercado.

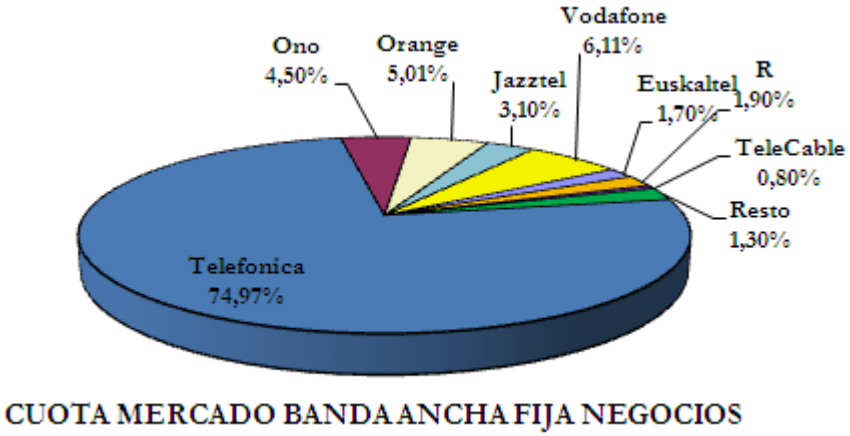


Gráfico 4.1.14 Porcentaje de cuota de mercado de los operadores en banda ancha empresarial. Fuente: Informe CMT 2012. Elaboración propia

Por otro lado, el segmento residencial sí estuvo más repartido. **Aquí, Telefónica experimentó una pérdida de cuota, que pasó del 43,3% del año 2011 al 41,8%.** El resto de los operadores más o menos mantuvieron sus cuotas de mercado.

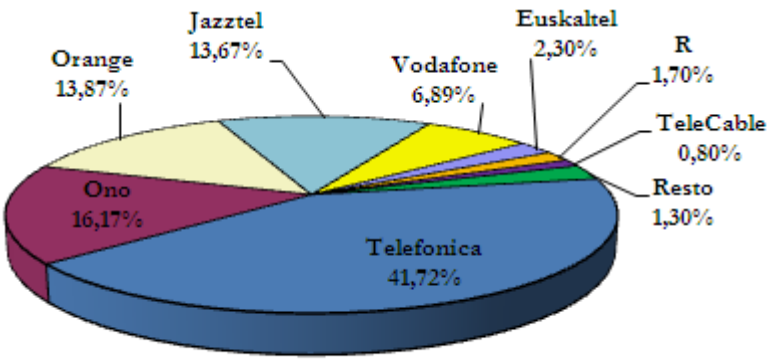


Gráfico 4.1.15 Porcentaje de cuota de mercado de los operadores en banda ancha residencial. Fuente: Informe CMT 2012. Elaboración propia

4.1.2.5.4 Banda Ancha Móvil

El siguiente gráfico muestra las **cuotas de mercado** de los distintos operadores en relación al total de líneas de banda ancha móvil, tanto en el caso de **dispositivos de voz y datos (teléfonos móviles) como en el de líneas exclusivas de datos (módems USB). Movistar sigue líder del mercado pero los operadores Yoigo y las OMV ya alcanzan una cuota de 18,8%.**

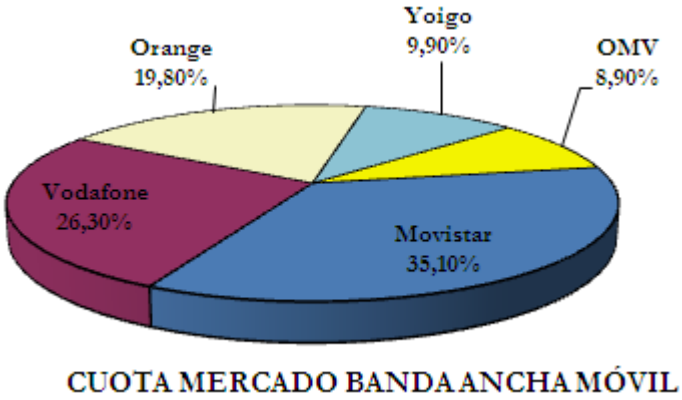


Gráfico 4.1.16 Porcentaje de cuota de mercado de los operadores en banda ancha móvil. Fuente: Informe CMT 2012. Elaboración propia

4.1.3 Situación de los servicios mayoristas

El servicio de **alquiler de circuitos** en el ámbito mayorista es el que se prestan entre sí los operadores para proporcionar una cierta capacidad de transmisión entre dos puntos debido

a que no todos tienen infraestructura propia para ofrecer un servicio. En este apartado se incluyen de forma agregada los datos de las líneas troncales, de las terminales y de las utilizadas para la conexión de salas **OBA (Oferta del Bucle de Abonado).**

Respecto al acceso al bucle de abonado, **Telefónica es el único operador que tiene una red con cobertura nacional** a través de la cual puede ofrecer servicios de banda ancha. La regulación establece que **Telefónica tiene la obligación de facilitar el acceso a esa red a los operadores alternativos** que quieran dar servicios de banda ancha. Para ello existen dos fórmulas: **desagregando el bucle de abonado y los accesos indirectos. Para más obtener mas información sobre los tipos de servicios mayoristas anteriormente comentados consultar el documento memoria_anex.pdf apartado ANEXO3.**

En relación con los servicios mayoristas de acceso de banda ancha, en 2010 se definió un nuevo servicio de acceso indirecto Ethernet de banda ancha (NEBA), que sustituirá progresivamente a los actuales, facilitará acceso mayorista a la nueva red de fibra de Telefónica y que anteriormente en el proyecto se definió en qué consistía detalladamente y las mejoras que supondrá.

4.1.3.1 Líneas

La ganancia de nuevos accesos por parte de los operadores alternativos se reflejó en los mercados mayoristas de banda ancha con un **aumento de los bucles desagregados y de las líneas contratadas** del servicio de concentración IP. En este último servicio de acceso indirecto a la banda ancha, continuó el incremento de líneas iniciado a finales del año 2009 como consecuencia de las medidas regulatorias introducidas por la CMT que supusieron una **reducción de los precios de los servicios de acceso indirecto y la introducción de nuevas modalidades de ofertas mayoristas** que permitían a los operadores la contratación de la banda ancha sin el servicio telefónico de Telefónica. De este modo, la modalidad de concentración IP **(ADSL IP) presentó un incremento del 38,4%.** La modalidad de concentración ATM o **GigADSL descendió un 3,3%.** Finalmente, el servicio de reventa descendió el 10,1%.

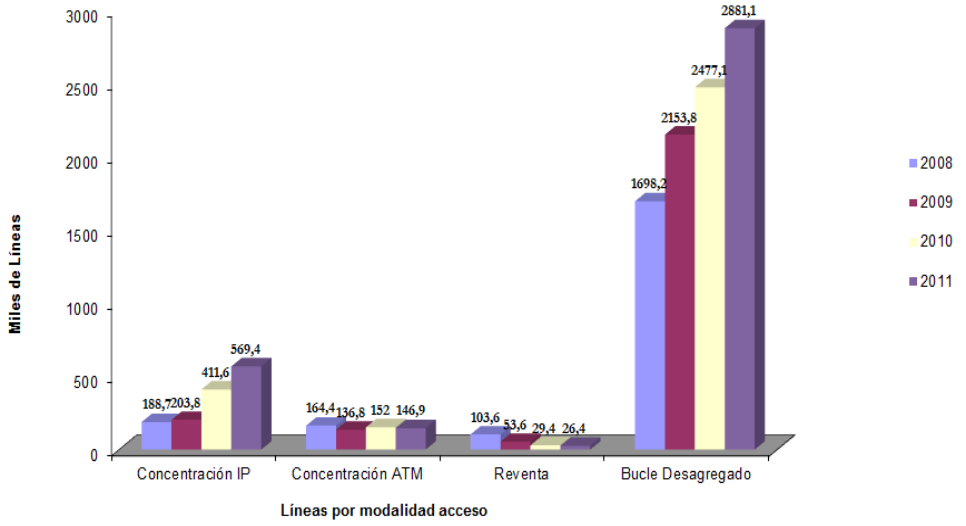


Gráfico 4.1.17 Líneas por modalidad de acceso a la banda ancha mayorista.
Elaboración propia .Fuente: Informe CMT 2011

4.1.3.2 Cuotas de mercado

Telefónica mantuvo el liderazgo en el mercado del servicio de circuitos a nivel mayorista, con un **83,2%** del total de ingresos. Los **operadores alternativos vieron reducida** su cuota a nivel consolidado aun cuando Ono, Orange y Grupo Abertis mantuvieron sus cuotas, del 4,2%, 2,6% y del 2,4%, respectivamente.

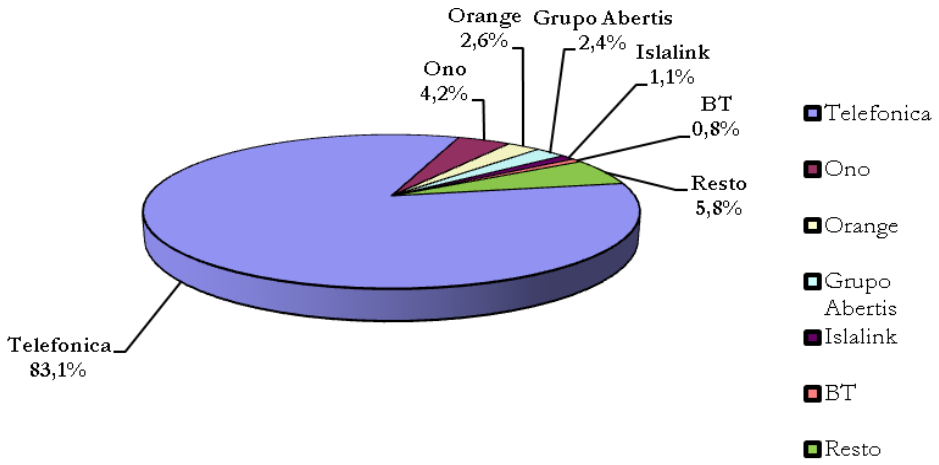


Gráfico 4.1.18 Cuotas de mercado por ingresos de circuitos alquilados a operadores.
Elaboración propia .Fuente: Informe CMT 2012

4.2 TENDENCIAS Y USOS DE LAS TECNOLOGÍAS EN ESPAÑA

Una vez realizado un análisis en materia económica y de evolución de líneas y cuotas de mercado cabe realizar un estudio sobre el uso que hacemos de las tecnologías para comprender las tendencias de la sociedad, de conocer al usuario, sus preferencias, sus hábitos…, porque marcaran la evolución de los servicios.

Como viene siendo habitual, la digitalización de nuestra vida es un hecho y que cada vez dependemos en mayor medida de lo digital y de Internet para la realización de nuestras actividades más cotidianas. Así, la forma en la que nos comunicamos con nuestros amigos, nos informamos, o incluso nos relacionamos con las Administraciones, se ha ido adaptando para incorporar las nuevas posibilidades que ofrece Internet que en muchos casos modifica los comportamientos de los ciudadanos.

El año 2012, desde el punto de vista de la evolución del mundo digital, la **Banda Ancha Móvil que crece más de un 150%,** impulsada sobre todo por el personal más joven. Este incremento ha sido posible **gracias al desarrollo del mercado de los smartphones**, con nuevos modelos de altas capacidades que permiten el acceso a los servicios de forma cómoda y fácil. **Por estos motivos, se puede considerar que el smartphone ha sido el dispositivo destacado de 2012.**

Dentro de los servicios en los que se ha observado una **mayor evolución durante el año 2012** se encuentra la **mensajería instantánea**, que ha destacado por el incremento en su nivel de penetración, valoración y el número de los que lo utilizan con frecuencia diaria (98% de incremento con respecto a los datos de un año antes). También aumenta el **número de usuarios que se conectan diariamente**, e incluso que se encuentran conectados en todo momento.

El en 2012 se ha consolidado el aumento del **consumo de la modalidad de acceso online (streaming)**, aunque se sigan descargando contenidos. Dicho aumento se deba posiblemente a la aceptación del concepto de cloud. Todos estos hechos anteriormente comentados pasó a describirlos más detalladamente en los siguientes párrafos.

4.2.1 Tecnologías empleadas para el acceso a Internet

El acceso a Internet se ha venido produciendo durante años de una manera exclusiva mediante tecnologías fijas, inicialmente mediante banda estrecha por el mismo par de cobre que la telefonía fija utilizando un módem, y posteriormente sobre este mismo par de cobre adaptándolo a la tecnología xDSL, mediante cable o fibra. Ahora, en la actualidad, ya existen en el mundo **el doble de subscripciones de banda ancha a Internet mediante tecnologías móviles que mediante tecnologías fijas.**

Para estudiar la utilización de los diferentes tipos de banda ancha por parte de los usuarios se puede clasificar con tres perfiles a los usuarios: solo acceso fijo, solo acceso móvil y acceso fijo y móvil. Se observa como el primer grupo es todavía el grupo más importante con un 60% del total de internautas, aunque **cada vez gana más peso el grupo de los que utilizan ambas tecnologías de acceso (34%)** e incluso los que utilizan **solo tecnologías móviles (5,2%)**.

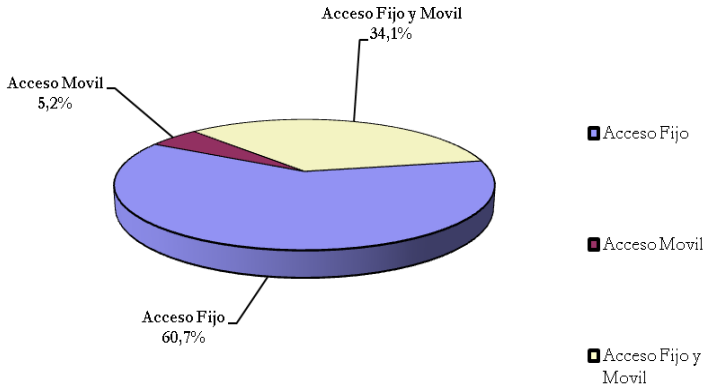


Gráfico 4.2.1 Utilización de la tecnología de acceso. Elaboración propia .Fuente: Informe Sociedad Información 2012 Telefónica

Los usuarios solamente de acceso fijo se conectan mayoritariamente solo desde casa (76,2%), mientras que los usuarios de acceso fijo y móvil se conectan desde cualquier ubicación (73,6%), y cabe destacar como **dos tercios de los usuarios de solo acceso móvil se conectan solo desde casa**.

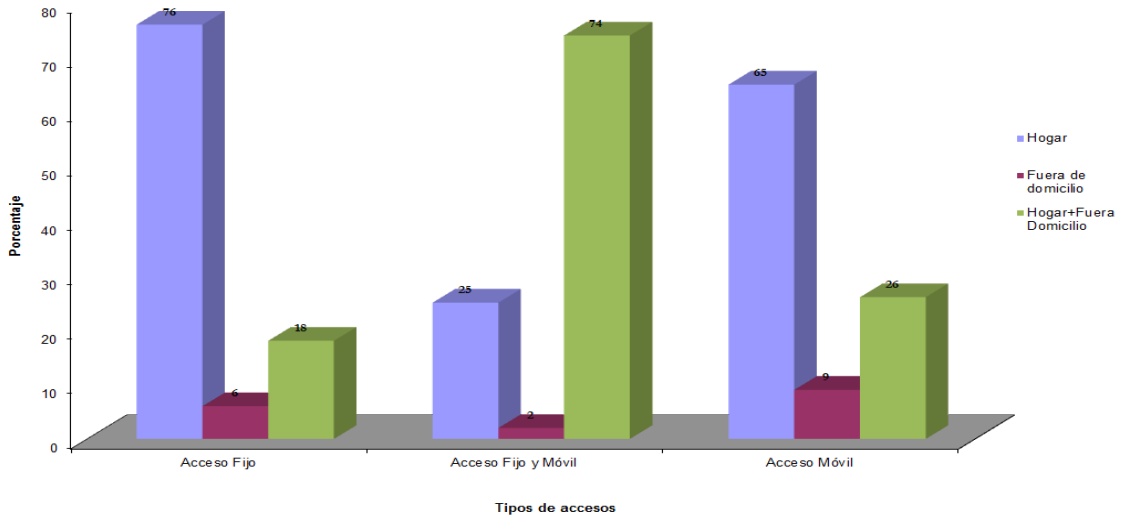


Gráfico 4.2.2 Lugar de uso de Internet según tecnología de acceso. Elaboración propia .Fuente: Informe Sociedad Información 2012 Telefónica

4.2.2 Dispositivos empleados para la conexión a Internet

En 2011, el ordenador portátil ha desbancado por primera vez al ordenador de sobremesa como principal medio para acceder a Internet desde los hogares españoles, de este modo, algo más de dos de cada tres hogares españoles utilizan este dispositivo para acceder a la Red. **El PC sigue siendo un año más el dispositivo central de acceso a Internet,** pero realmente, **el motor de dicho crecimiento ha sido el teléfono móvil**, con un crecimiento de 29,4 puntos porcentuales hasta ser utilizado por el 43,4% de los internautas**, lo que supone un 210% más de uso con respecto a los datos del año anterior**. También en el 2012, el uso de la **tablet** ha aumentado más de un **500%,** aunque todavía es utilizado solamente por el 2,7% de los internautas.

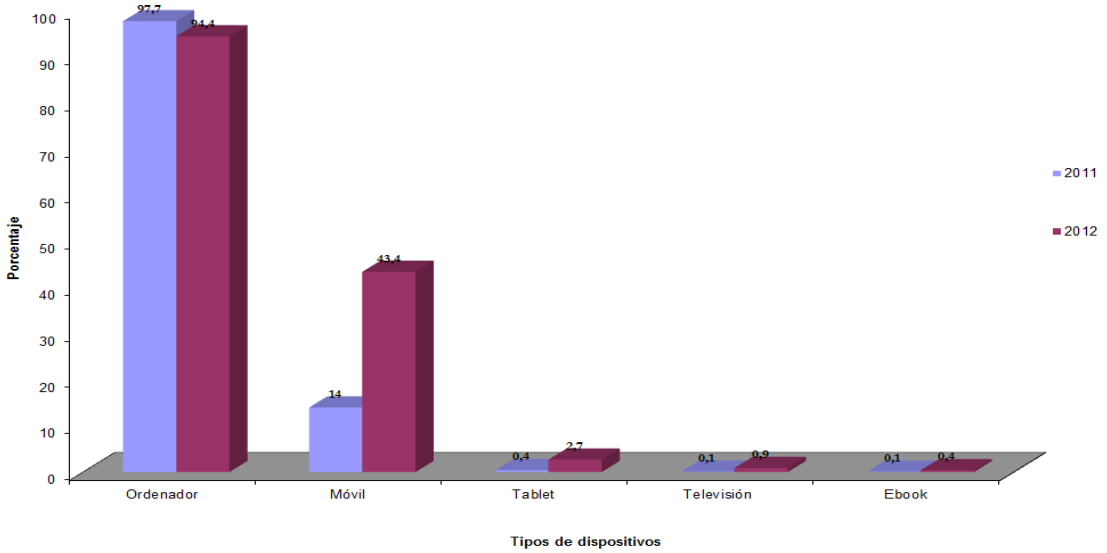


Gráfico 4.2.3 Evolución del dispositivo de acceso a Internet. Elaboración propia .Fuente: Informe Sociedad Información 2012 Telefónica

Cabe mencionar también, que uso de la banda ancha móvil con respecto a la banda ancha móvil-Wifi que realizan los usuarios desde los teléfonos móviles, antes se utilizaba principalmente las redes WiFi a la hora de conectarse a Internet, pero esta ha cambiado durante el último año y **la banda ancha móvil** ha crecido 20 puntos porcentuales entre los internautas que se conectan mediante el móvil hasta **convertirse en el primer medio de acceso**, además aumenta el número de usuarios que utilizan ambas formas de conectarse hasta el 40%.

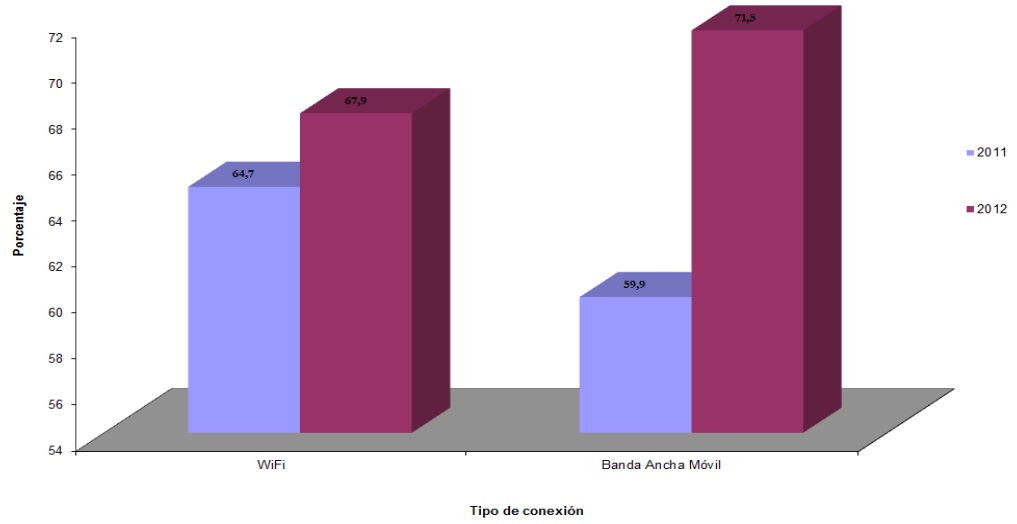


Gráfico 4.2.4 Tecnología de acceso desde el móvil. Elaboración propia .Fuente: Informe Sociedad Información 2012 Telefónica

Indicar que dos de cada tres internautas poseen un smartphone y uno de cada seis tiene una tablet. Este tipo de equipamiento ha **doblado su tasa** de penetración con respecto al año 2011.

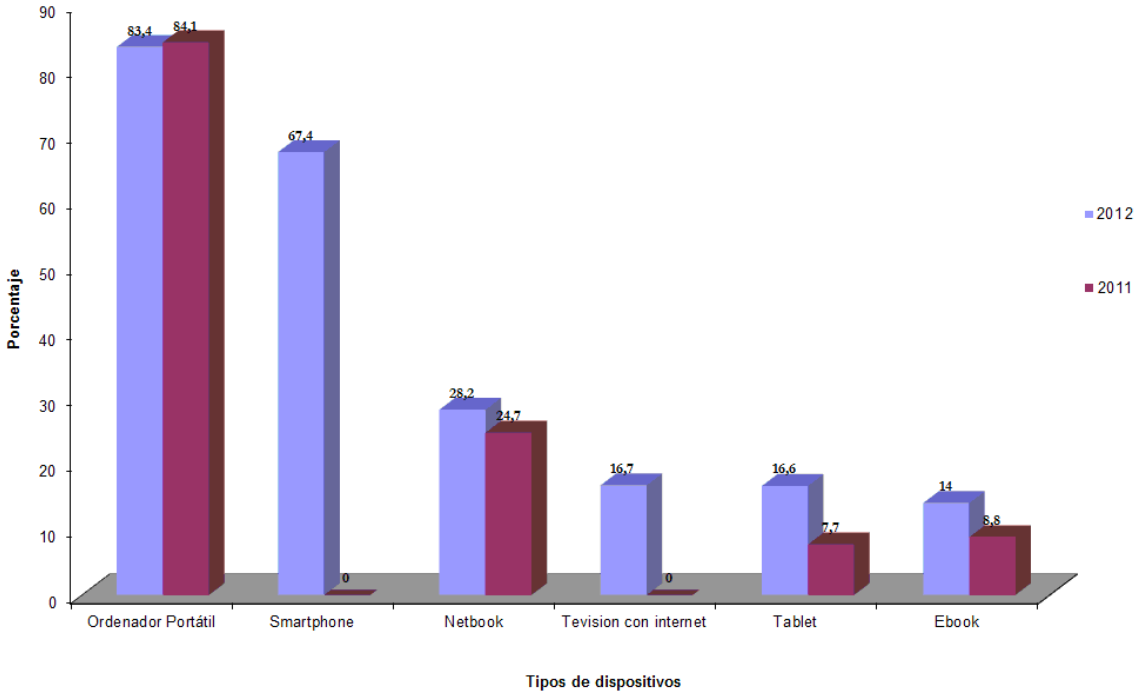


Gráfico 4.2.5 Equipamiento de los usuarios de Internet de España sobre el % total de internautas. Elaboración propia .Fuente: Informe e2012 de la Fundación Orange

4.2.4 Actividades realizadas a través de Internet

Las actividades mas utilizadas **por los jóvenes son las actividades multimedia y buscar información con 20 puntos de diferencia con el resto de internautas**. Para el resto de actividades, no existe una mayor diferencia destacable entre jóvenes y el resto de usuarios.

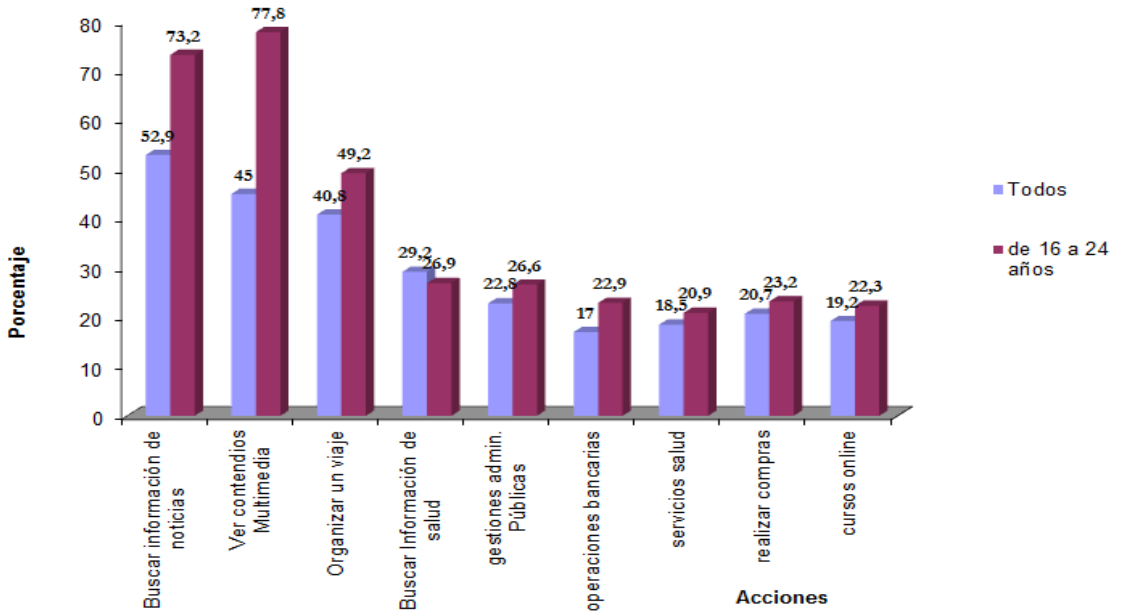


Gráfico 4.2.6 Realización de actividad usando Internet. Elaboración propia .Fuente: Informe Sociedad Información 2012 Telefónica

4.2.5 Contenidos a los que acceden los ciudadanos

El **tipo de contenido más accedido en todos los segmentos de edad son las películas y las series**, que son consumidas por el 97,4% de los usuarios. Además, **los internautas son más propensos a la lectura**, tanto utilizando el formato físico papel como el resto de formatos alternativos como el ordenador portátil, el e-reader e incluso el móvil.

Otro contenido para el que el grado de adopción depende de la edad es el de **navegar y búsqueda de información**, que se conforma como el segundo tipo de contenido entre los jóvenes y el cuarto a nivel global. En el **acceso a deportes**, pero en este caso según el género, con un acceso del 93% en el caso de los hombres y del 46,8% entre las mujeres, que es prácticamente la mitad.

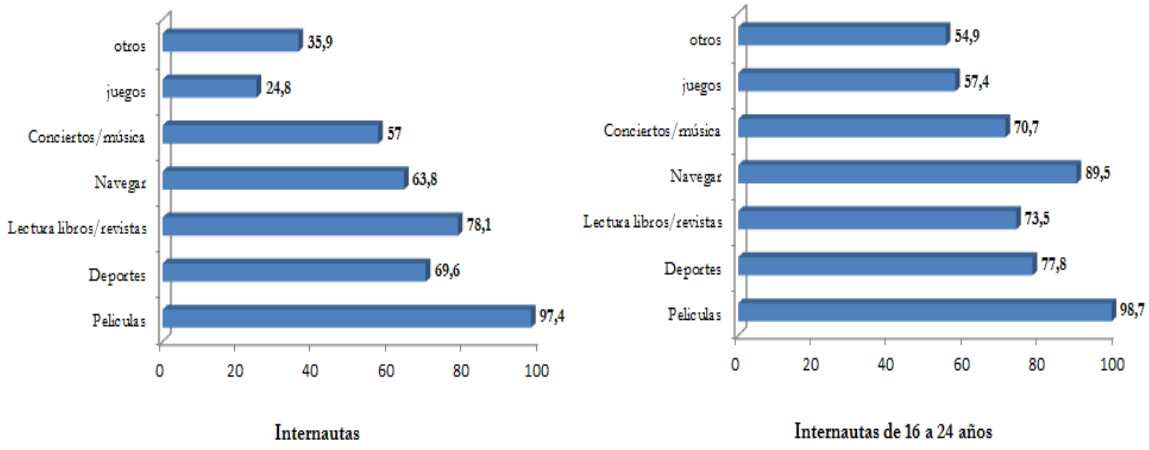


Gráfico 4.2.7 Contenidos a los que acceden los ciudadanos. Elaboración propia .Fuente: Informe Sociedad Información 2012 Telefónica

La mejora de las redes de comunicación, ha permitido que ya durante el año 2011 el uso de las descargas y del acceso online vía streaming fuese similar. Y durante el 2012 los datos muestran como un gran número de internautas, el 40%, utilizan ambos medios; sin embargo entre los que utilizan solamente una de las dos modalidades, el **acceso mediante streaming se impone claramente a la descarga** con un 19,5% frente a un 8,1%.**Respecto a la música**, un 33,8% de los internautas descargan música mientras que un 39,3% se decantan por su uso vía **streaming**. Destaca como Youtube es el primer sitio al que recurren los usuarios para acceder a música (46,5%), seguido por Spotify (27,2%).En cuanto **al video**, también hay **un mayor uso en la modalidad de streaming** tanto en penetración, 48,5% frente a 26,3%.

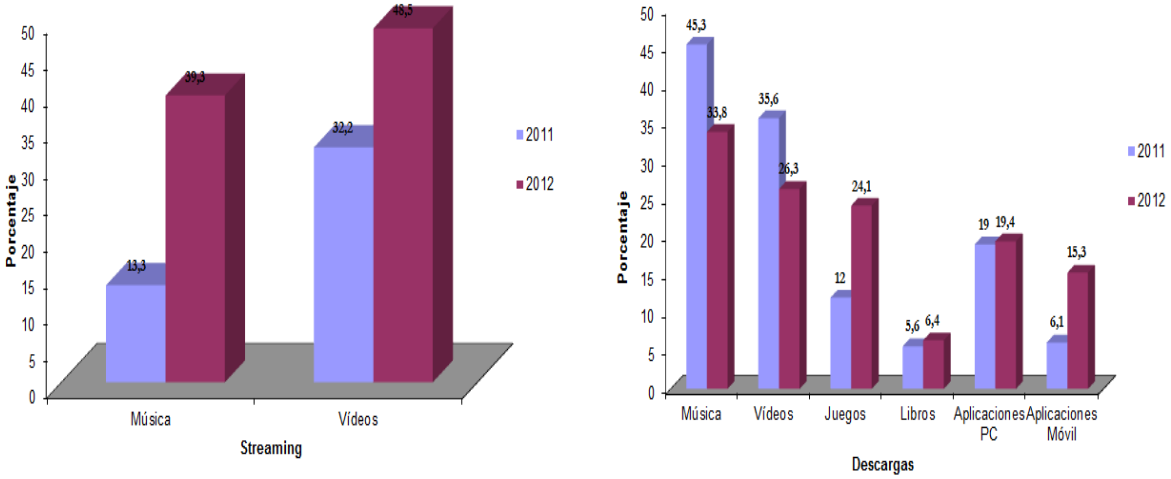


Gráfico 4.2.8 Evolución de los distintos servicios de descarga y streaming. Elaboración propia .Fuente: Informe Sociedad Información 2012 Telefónica

4.2.6 Métodos de comunicación empleados por los ciudadanos

De entre los diferentes usos de Internet, empieza a despuntar su **utilización como medio para comunicar personas**, y ya **cuatro de cada cinco internautas lo utiliza con este fin**, mientras que entre los más jóvenes esta cifra sube hasta **93,4%. La comunicación mediante llamada de móvil es la preferida en todas las edades.** Destacar que aumenta bastante el método de comunicación mediante **mensajería instantánea hasta 83%** gracias a aplicaciones como Whatsapp o Line.

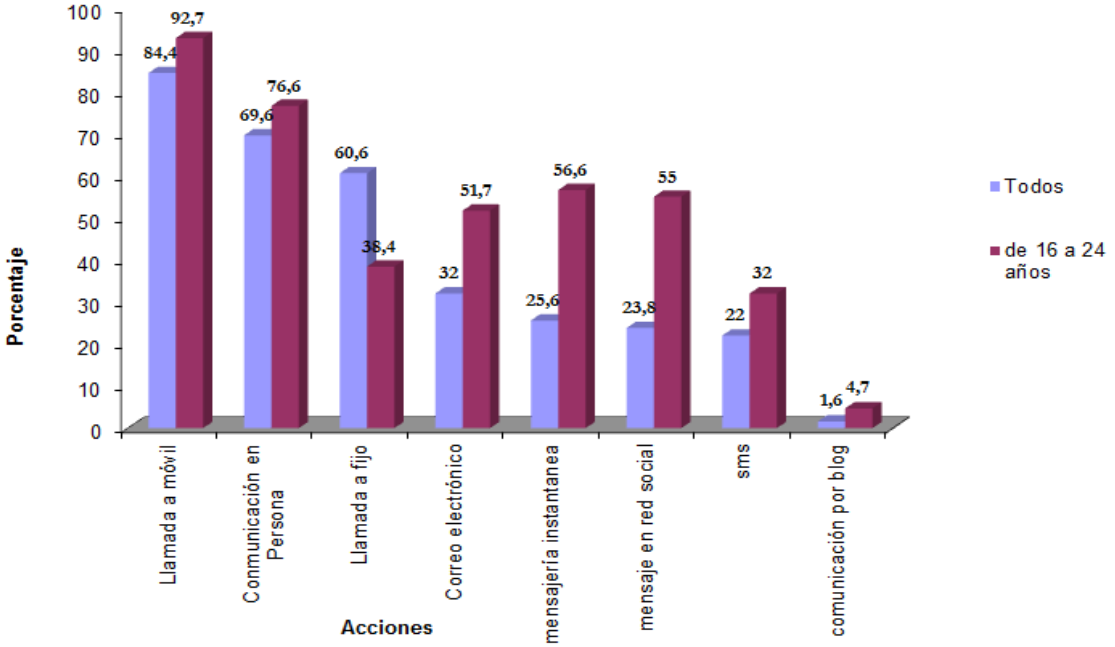


Gráfico 4.2.9 Métodos empleados para comunicarse. Elaboración propia .Fuente: Informe Sociedad Información 2012 Telefónica

España cuenta con **20 millones de usuarios de WhatsApp de los 300 millones que hay en todo el mundo**. Unos datos muy elevados si se comparan con el número de población total del país y si lo comparamos con otros mercados. Los elevados precios de los SMS y la masiva adopción de teléfonos inteligentes tienen la culpa de que **España sea uno de los territorios predilectos de este servicio**. Unos 31.000 millones de mensajes de Whatsapp van y vienen en un solo día. La aplicación Whatsapp es una de las herramientas más utilizadas por los usuarios de smartphones, cada vez más adictos a su uso, puesto **que lo miran de media 150 veces al día**, según un reciente estudio de TomiAhonen Almanac. De hecho, Whatsapp puede llegar a enviar 11.000 millones de mensajes y recibir 20.000

millones al día. Por si esto no fuese suficiente, se comparten un total de 325 millones de fotos durante un solo día. Junto con España, países como Alemania, México o India también alcanzan la cifra de 20 millones de usuarios, según ha revelado la compañía. Son algunos de los territorios donde el servicio de mensajería es especialmente popular y juntos aglutinan casi un tercio de la base de usuarios total. Resulta curioso que **nuestro país tenga tantos usuarios de WhatsApp como Alemania, que casi nos duplica en número de habitantes** (46 millones en España frente a 82 millones en Alemania, aproximadamente) o India, que supera los 1.200 millones, aunque la India todavía es un mercado emergente en el que la presencia de smartphones aún es reducida.

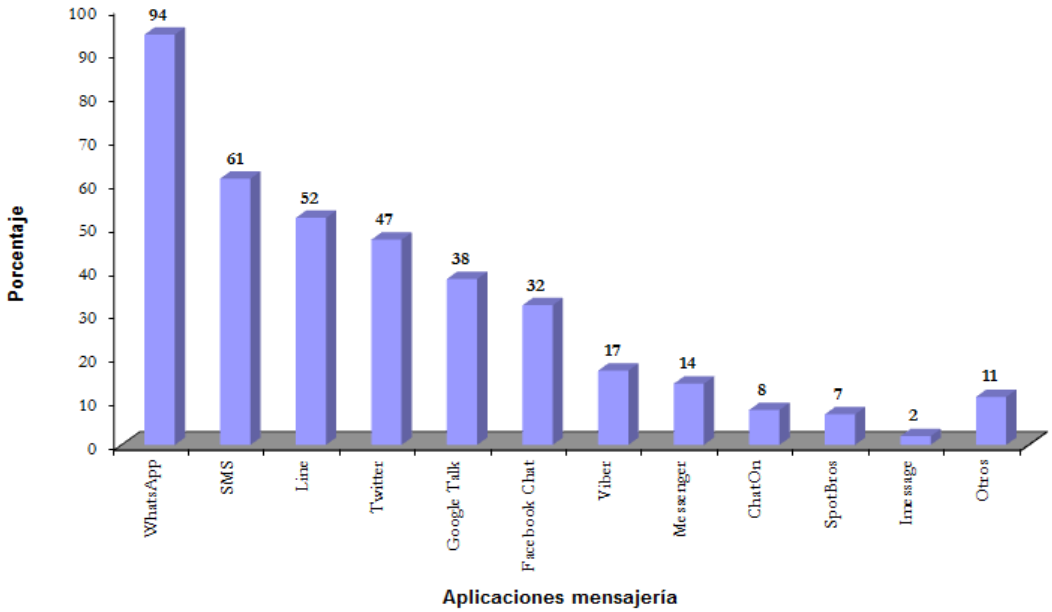


Gráfico 4.2.10 Software de mensajería instantánea utilizado. Elaboración propia .Fuente: Informe Sociedad Información 2012 Telefónica

4.2.7 Comercio Electrónico

A pesar de la crisis económica, el comercio electrónico ha experimentado un fuerte crecimiento en España en 2012. El número de personas que han realizado algún tipo de compra a través de Internet en los últimos doce meses ha aumentado casi un 12% con respecto al año 2011. Un año más, **el producto más demandado a través de Internet son los paquetes vacacionales** y los viajes, que fueron adquiridos en alguna ocasión por la mitad de los compradores españoles. Por el contrario ha bajado casi 10 puntos los servicios para viajes respecto a 2011.

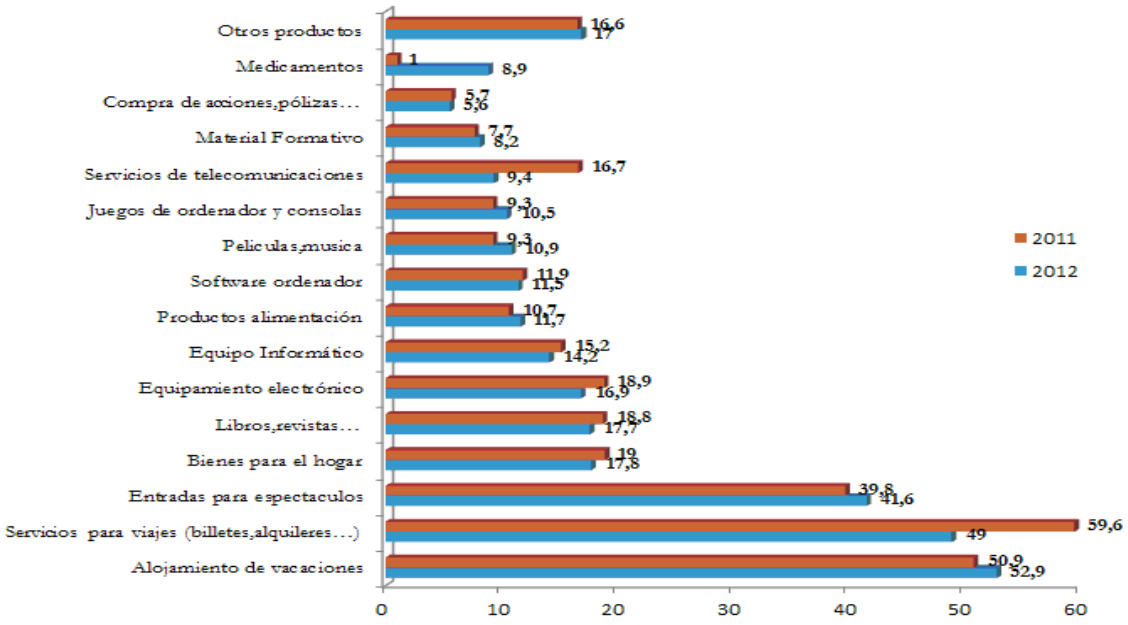


Gráfico 4.2.11 Productos y servicios adquiridos por Internet. Elaboración propia .Fuente: Informe e2012 de la Fundación Orange

El **principal medio de pago** utilizado por los internautas españoles en la realización de sus compras a través de Internet **sigue siendo la tarjeta de crédito o de débito**. Sin embargo, cabe indicar que los **medios tradicionales están perdiendo cuota de mercado**. El **pago a través del teléfono móvil sigue siendo testimonial**, ya que apenas es utilizado por el 1%. Se espera que la paulatina incorporación de la tecnología NFC al móvil fomente el pago con este dispositivo en los próximos años.

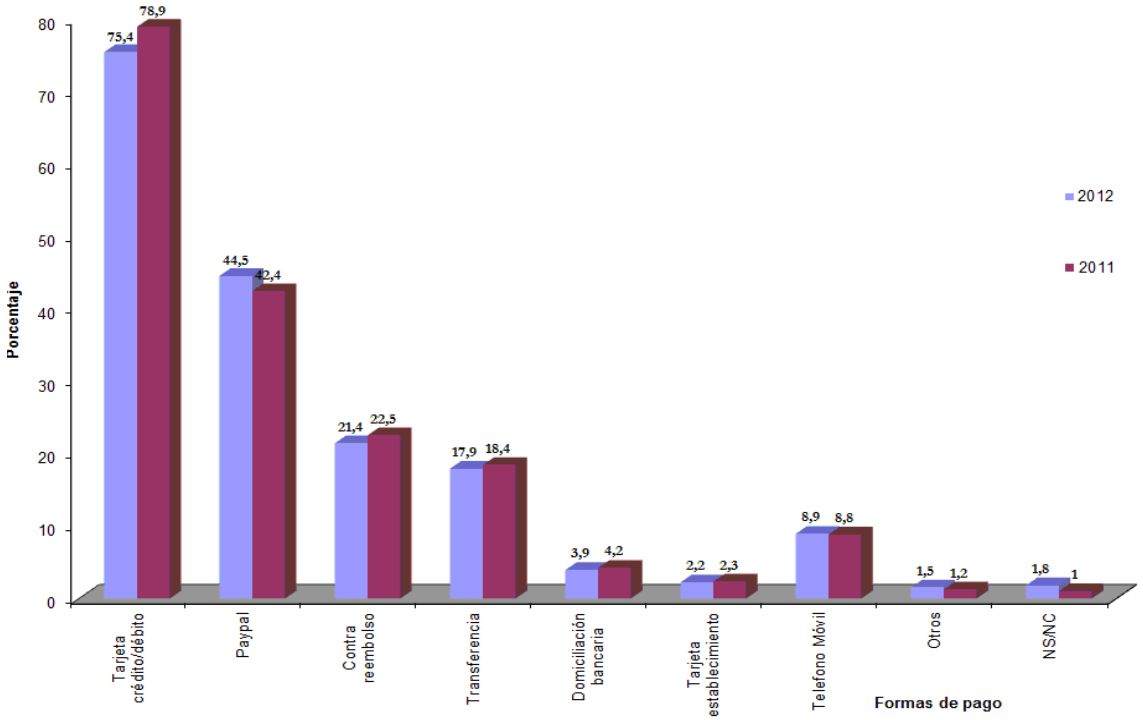


Gráfico 4.2.12 Forma de pago empleado para las comprar por Internet. Elaboración propia .Fuente: Informe e2012 de la Fundación Orange

4.2.8 Utilización de las redes sociales

Las redes sociales son sin duda uno de los fenómenos más importantes. Así, en un espacio breve de tiempo han pasado de ser servicios desconocidos, a ocupar los primeros puestos entre los servicios de Internet en cuanto al número de usuarios y el tiempo dedicado por ellos. Durante el año 2012 se observa que la penetración de las redes sociales crece en **6,5 puntos porcentuales hasta alcanzar el 63,7% de los internautas**.

Tuenti es la red social preferida por los más jóvenes (entre 14 y 19 años), con un 60,2% de penetración, 10 puntos por encima de Facebook. En cuanto al crecimiento **Twitter se presenta como la red que muestra la mayor tasa de crecimiento durante el último año**, un 175% a nivel global y un 240% entre los más jóvenes.

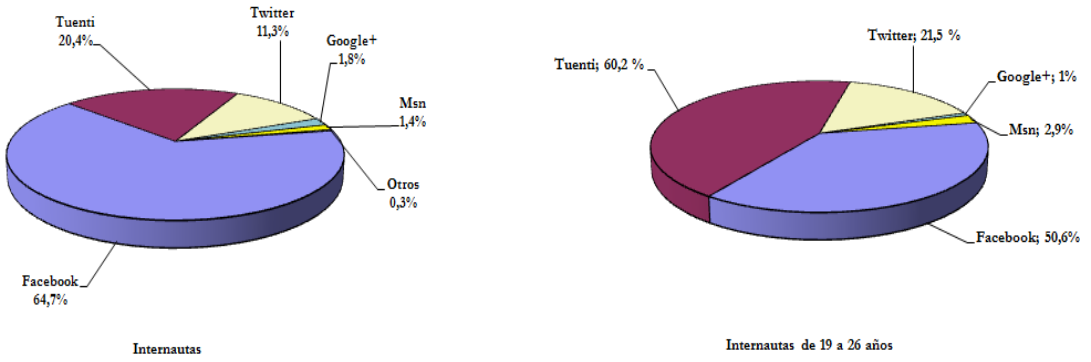


Gráfico 4.2.13 Penetración de las diferentes redes sociales. Elaboración propia .Fuente: Informe Sociedad Información 2012 Telefónica

5 FUTURO DE LAS REDES Y TECNOLOGÍAS

A lo largo de las últimas décadas, las tecnologías de red han pasado por distintas olas de innovación con sus correspondientes propuestas sobre arquitecturas, protocolos e interfaces. Entre ellas hay que destacar SNA, X.25, Ethernet y el omnipresente TCP/IP. La conmutación de circuitos y la de paquetes o los modelos híbridos como ATM. También las redes por cable, la fibra y por ondas de radio. Una de las **mayores dificultades** para el despliegue de las nuevas redes reside en que **el protocolo Internet fue diseñado para las aplicaciones de red fija** y no se tuvieron en cuenta las características del canal radio, que es el que, cada vez más, se utiliza para el transporte de las aplicaciones y servicios. Por ello, el gran objetivo es ahora **desarrollar redes con alta calidad de servicios**, que tengan, además, una mayor **flexibilidad y capacidad (ancho de banda)** de tal forma que las aplicaciones del futuro no estén limitadas. Por otra parte, sigue siendo necesario un esfuerzo en el desarrollo de soluciones más económicas también para los accesos de fibra, para permitir nuevos despliegues que permitan la extensión de los servicios de video que precisan **sistemas con anchos de banda mucho más elevados** que los que están actualmente disponibles.

Los servicios digitales actuales, fundamentalmente los servicios de vídeo y cloud, están cambiando la naturaleza determinística de la demanda de tráfico en las redes, es decir, cada vez es más complejo tener certeza de lo que va a suceder. Por ello, **se hace complicado determinar de manera fiable los requisitos de tráfico que han de poder cursarse por**

las redes de telecomunicación. La red de transporte de un operador es especialmente sensible a estos cambios, ya que en su implementación actual, cualquier modificación implica la operación y actuación en múltiples sistemas, lo que supone importantes retardos (incluso meses) en la provisión de servicios finales. A este segmento de red **se le exigen tres características** principales:

- **Alta capacidad** para poder congregar y transportar el tráfico de todos los usuarios y servicios.
- **Flexibilidad.**
- **Eficiencia** que permita usar el camino más adecuado para transportarlos de un sitio a otro.

Las arquitecturas actuales de las redes de transporte fueron concebidas y diseñadas teniendo en cuenta tanto las características, como la demanda de tráfico de los servicios de comunicación tradicionales (básicamente la voz). Sin embargo, **los servicios digitales actuales** (fundamentalmente los de vídeo y el *cloud computing*) **están cambiando la naturaleza de la demanda de tráfico** de las redes. Y en este sentido están teniendo lugar dos tendencias:

- La **demanda de tráfico en general se está incrementado de manera notable**.
- **El tráfico se está haciendo cada vez más variable,** es decir, su comportamiento se está convirtiendo en una magnitud cada vez menos predecible, con lo que no es sencillo planificar las redes de manera óptima y, sobre todo, de manera eficiente.

5.1 PREVISIÓN DE INCREMENTO DE LA DEMANDA DE TRÁFICO

La explosión de servicios digitales, fundamentalmente el vídeo y los servicios de cloud, están incrementando de manera notable el consumo de tráfico que se realiza a través de las redes, tanto fijas como móviles. Además, esta demanda de tráfico es variable, por lo que dimensionar las redes de la manera óptica es cada vez más complejo. Según las previsiones **el crecimiento interanual en el periodo 2012-2017 del volumen global de tráfico móvil se situaría en torno al 40%.**

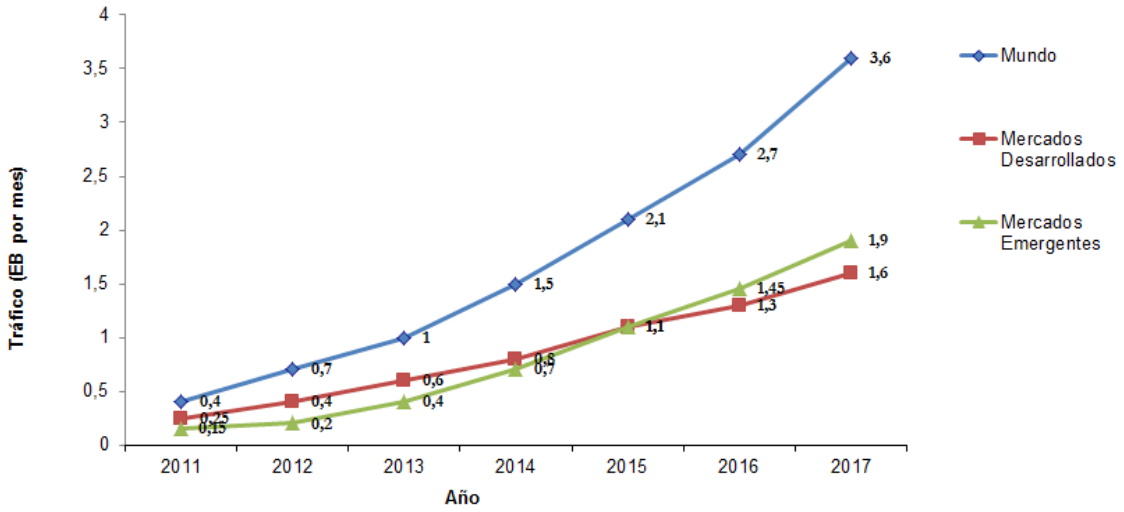


Gráfico 5.1.1 Previsión del volumen global de tráfico de móvil .Elaboración propia. Fuente: Juan Pedro Fernández-Palacios, Junio 2013, Estrategia de Negocio y Tecnológica

Desde el punto de vista del tráfico total de Internet, las previsiones apuntan a que en **2016 el tráfico IP global que circulará por las redes será de 110 Exabytes al mes**. En el caso concreto del tráfico de usuarios finales, **el crecimiento interanual medio desde 2011 se prevé que sea del 32%**. Y la mayor parte de este crecimiento vendrá de la mano del tráfico de vídeo, lo que tiene una importante implicación, ya que el patrón de tráfico del vídeo es mucho más dinámico que el del resto de tráfico.

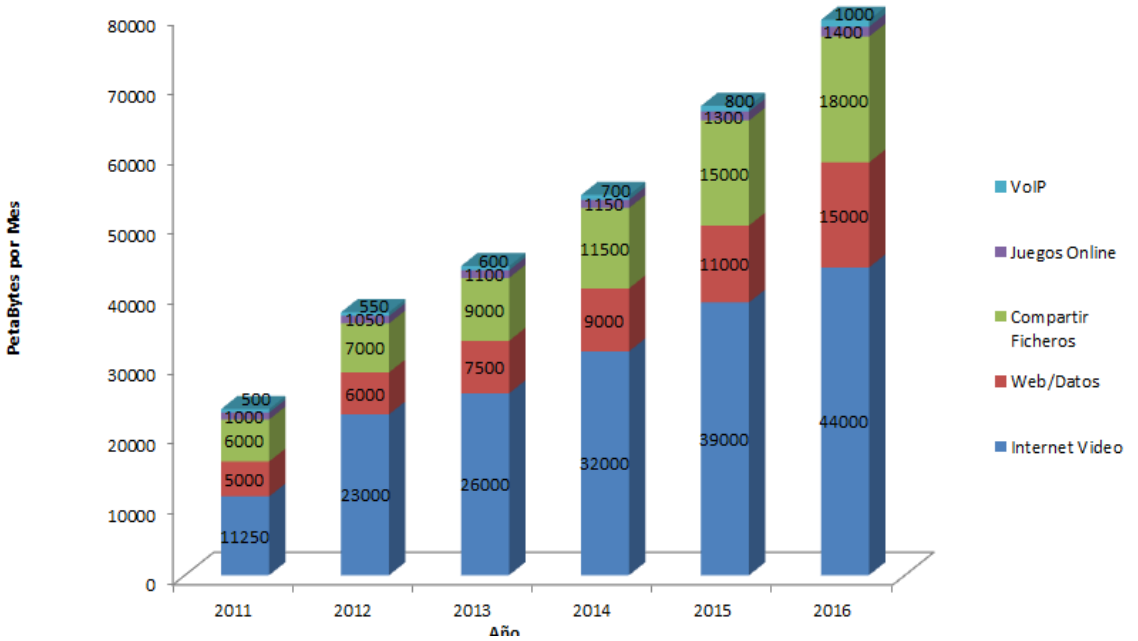


Gráfico 5.1.2 Previsión del volumen total del tráfico de Internet .Elaboración propia. Fuente: Cisco VNI Global Forecast 2013

Está claro que para responder a la demanda en este nuevo contexto que imponen los servicios, **la red de transporte debe ser elástica**. Es decir, la red debe **ofrecer mecanismos para que la provisión de los servicios de conectividad se realice de una manera dinámica** y se **atiendan los requerimientos elásticos de la demanda de tráfico cambiante**. Se trata de proporcionar un **control de conectividad automático,** de manera que los recursos de la red sean usados de manera dinámica y que, además, incluso la propia configuración de la red se realice de una manera óptima basándose en la información que proporcionan los servicios digitales, como por ejemplo los de cloud.

El **incremento de la capacidad** puede ser alcanzado mediante el uso intensivo de **tecnologías de transporte fotónico**, la **automatización** puede ser conseguida transfiriendo funcionalidad desde los sistemas de gestión de red a los **mecanismos de señalización estándares de las redes**. La evolución hacia esta red de transporte flexible y moldeable prepara el camino hacia una arquitectura única de provisión de red, que lleva a una reducción de costes y a una mejora en la provisión de servicios. En esta evolución, **el concepto SDN (Software Defined Networking),** aparece como una alternativa prometedora para la implementación de la provisión unificada, ya que se trata de definir redes vía software, es decir, virtualizar redes tal y como se hace en la actualidad en los Datacenters y que explico mas detenidamente en el punto 12.3

5.2 VIRTUALIZACION DE LAS REDES

En el punto 12.1 hacia mención a que para la creación de redes elásticas que se adapten a las necesidades futuras**, es necesaria la migración de las funcionalidades actuales de provisión de la red desde los sistemas actuales de gestión con el objetivo** de una **arquitectura de provisión de red unificada**. Es decir, si se **llevan las funcionales** que ahora se realizan vía sistemas, a los **propios equipos de la red** (incorporando dichas funcionalidades en su plano de control, es decir, en su señalización), **los mecanismos y las operaciones de red se simplifican**. El objetivo es que se pueden activar todos los elementos precisos para **provisionar un servicio de manera unificada**.Para conseguir este objetivo de simplificación hay ciertas tecnologías y elementos clave:

- Por un lado, **una interfaz que permita configurar la red**, es decir, sus elementos, **usando estándares que permitan simplificar los procesos**. Actualmente estos procesos de configuración se realizan a través de sistemas específicos que han sido

desarrollados para cada nodo de red y en los que se lanzan los comandos de configuración. Al final, el resultado es que se tienen muchos sistemas y muchos interfaces que implican complejos procesos, lo que deriva en un alto coste operativo y en un gran número de intervenciones humanas. **Tecnologías concretas como Openflow pueden ayudar a esta simplificación de la operación** minimizando el número de sistemas propietarios y ayudando por lo tanto a contener el OpEx.

- **Coordinar los recursos de la red y los data centre de acuerdo a los requisitos de los servicios** (como el Cloud). En este sentido el uso de **tecnologías SDN** puede facilitar esta tarea.
- Finalmente otro ingrediente **sería el API (Application Programming Interface) de servicios de red**, que abstrae la complejidad de la red y que ofrece capacidades de ésta a los servicios ya que API permite las funciones y procedimientos que pueden ser usados por otro software.

5.2.1 SDN: Redes definidas vía software

El modelo de red al que estamos acostumbrados, sobre el que se han desplegado todos los servicios y se han de basar los nuevos servicios digitales, considera **la red como un conjunto de dispositivos independientes**, asociados por medio de conexiones entre ellos, que transfieren datos de acuerdo con su estado interno. Las **funciones de un dispositivo de red** se dividen en **dos elementos principales**: **el plano de control y el plano de datos**. El **plano de control** engloba todas las funciones relacionadas con el establecimiento del **estado de la red y el trazado de la ruta** o rutas que deben seguir los datos. El **plano de datos** (en inglés también conocido como forwarding) comprende todos los procesos **relacionados con la entrega y recepción de los datos**. En los dispositivos de red actuales, el plano de datos se confía de manera casi exclusiva al hardware para obtener la máxima velocidad de conmutación. Las funciones del plano de control se encomiendan a un software específico para cada dispositivo, que utiliza algoritmos distribuidos para decidir cómo se gestiona cada paquete. Para que la red funcione correctamente, el software de cada dispositivo debe operar coordinadamente con los de todos los demás.

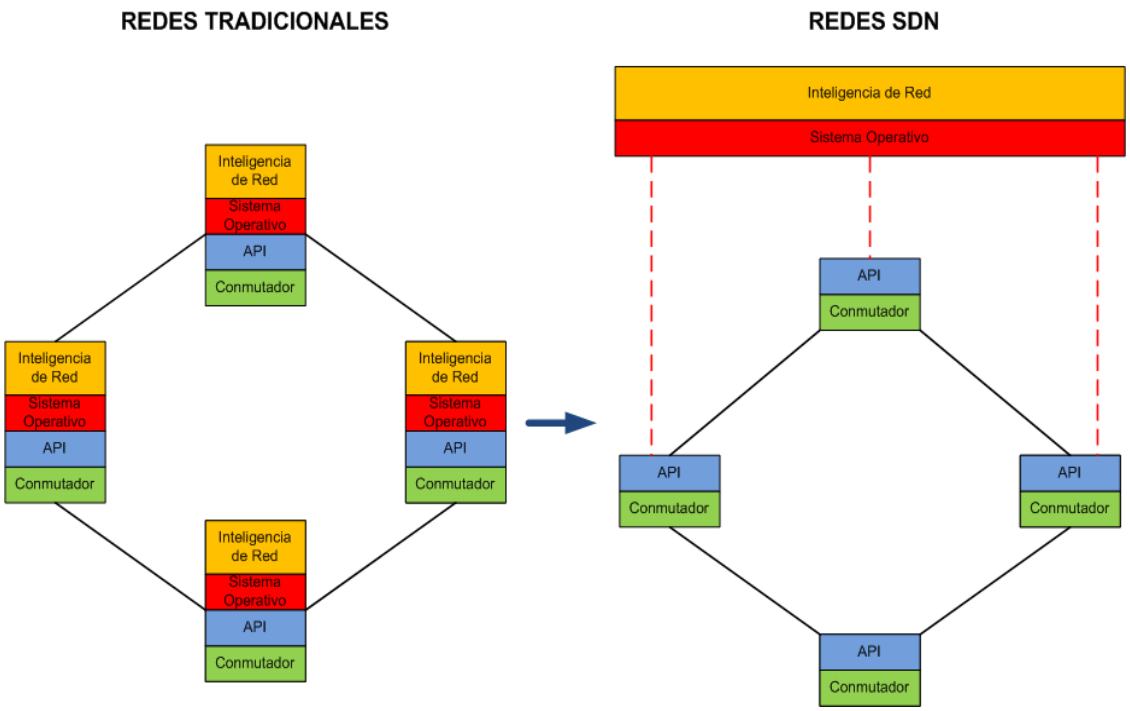


Figura 5.1.1 Redes tradicionales frente a redes SDN. Elaboración propia.

El concepto **SDN se sustenta sobre dos ideas principales**. La primera es la **separación radical entre el plano de control y el plano de datos**, hasta el punto de **ubicarlos en dos entidades diferentes** y, por lo general, separadas físicamente: el controlador, que se encarga de las funciones del plano de control, y los conmutadores (o switches), responsables de las del plano de datos. El uso del singular y el plural en las definiciones anteriores es completamente intencionado: aunque el modelo no lo exige, la solución más obvia consiste en tener un solo controlador que maneja varios conmutadores en un ámbito determinado. La segunda idea es la existencia de **un protocolo abierto entre controladores y conmutadores**, con el fin de que se puedan combinar con libertad elementos de distintos fabricantes para proporcionar las funciones de red, así como una interfaz abierta para el plano de control de manera que otros componentes que forman parte de la red, como pueden ser elementos de inteligencia de red o aplicaciones en general, puedan acceder al controlador de manera uniforme. En resumen, en **la SDN, las decisiones de control las adopta un elemento central**, mientras que las decisiones de conmutación las aplican los elementos distribuidos. Un **protocolo común permite que el controlador transmita sus decisiones a los conmutadores**. La existencia de este elemento central permite además abstraer la totalidad de la red en un elemento individual, encargado del comportamiento de la red en su conjunto.

5.2.1.1 Protoloco Openflow

El **protocolo OpenFlow** se basa en la idea de **que el controlador define unas reglas que luego aplican los conmutadores al recibir los paquetes**. Las reglas se activan al comprobar ciertas partes de los paquetes que van llegando y contienen acciones que tiene que ser aplicadas a dichos paquetes, como por ejemplo su reenvío a través de una ruta determinada, hacer algún cambio en ellos o incluso descartarlos.

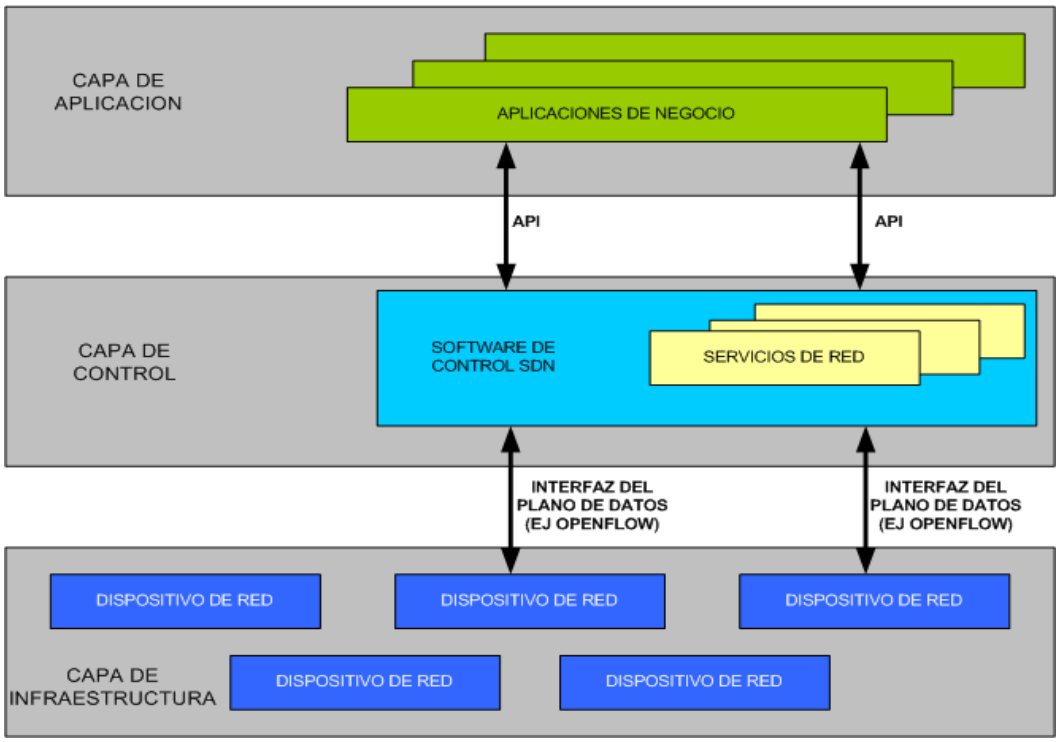


Figura 5.1.2 Arquitectura basada en el protocolo OpenFlow. Elaboración propia.

Este protocolo común permite que el controlador transmita sus decisiones a los conmutadores. La existencia de este **elemento central permite abstraer la totalidad de la red en un elemento individual**, con este protocolo actuando de manera similar a como lo hace el conjunto de instrucciones de un procesador, de manera que la red se convierte en una entidad programable, adecuada para ser controlada de la misma manera que otros elementos en una infraestructura de computación. Este es el aspecto fundamental del concepto SDN en general, posibilidades que ha podido contrastar el sector gracias al nacimiento del protocolo OpenFlow. Hay que recalcar que la **SDN es una tecnología aún en su fase inicial y que solo se ha empezado a explorar la superficie del profundo cambio que acarreará en la planificación y gestión de las redes**. Para

hacerse una idea, hay que pensar en el protocolo OpenFlow como si fuese el conjunto de instrucciones de procesamiento de un ordenador y en la posibilidad de aplicar al diseño y gestión de redes las mismas herramientas y técnicas que se usan en el desarrollo software: metodologías de diseño formal, lenguajes de alto nivel, compiladores e intérpretes, depuradores…

Por otro lado, **como se conoce mucho mejor el estado de la red desde el controlador**, resulta **viable compartir datos sobre ella**, tanto horizontal como verticalmente (con servicios y aplicaciones). En ambos sentidos del flujo de información, tanto entrante como saliente, es posible aplicar distintos niveles de abstracción de la información e incluso ocultarla si es necesario, lo que posibilita la aparición de nuevas modalidades de colaboración en el sector de los servicios de red; además, permite explorar nuevos patrones de integración y monetización. Con la ayuda de la SDN, **la red se convierte en un recurso de computación más**, muy similar a los otros, y susceptible de integración en una oferta general de servicios orientada a cubrir las necesidades de los clientes a todos los niveles

5.2.1.2 NFV: Virtualización de las funciones de red

NFV (Network Functions Virtualization) **son técnicas de virtualización de funciones de red permiten independizar las funcionalidades de la red de los equipos** que le dan soporte haciendo posible su **definición completa a través de software**, lo que **permite moldear los elementos de la red de manera sumamente flexible**. Al aplicar estas técnicas es posible además **sustituir el hardware específico por servidores de propósito general**, mucho más baratos y simplificar así toda la operación de esta infraestructura. Se trata de reducir las restricciones que impone el hardware específico de los equipos, de manera que la red pueda ser mucho más flexible, simple y escalable.

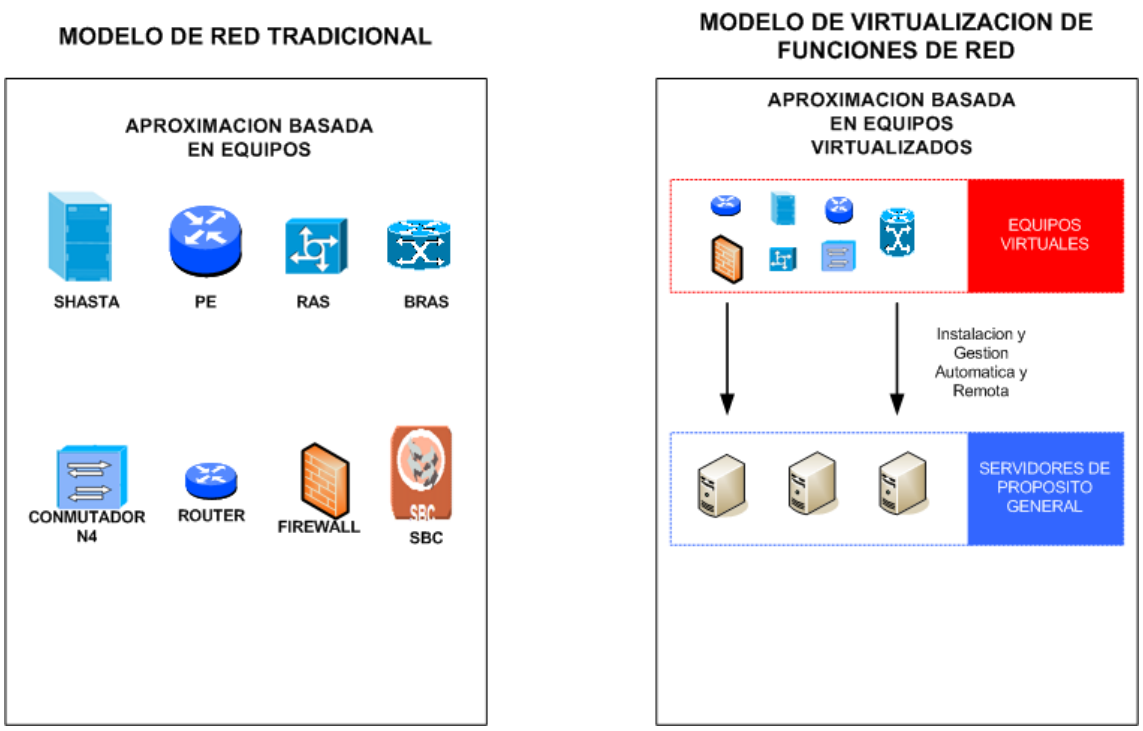


Figura 5.1.3 Modelo de red tradicional vs Modelo NFV. Elaboración propia.

Así, **tradicionalmente, los distintos roles y funcionalidades** que componen **una red** se han venido **basando en el uso de hardware específico**, dedicado en exclusiva a la realización de dichos procesos. Por ejemplo, cuando hablamos de un nodo de borde IP de acceso fijo está implícito que nos estamos refiriendo al mismo tiempo tanto a un rol desempeñado en la red. En este nuevo modelo, las ventajas no sólo vienen del ahorro por el uso de hardware de propósito general, sino por los beneficios de consolidación de funciones, ya que varias pueden estar en el mismo equipo y por supuesto, por la flexibilidad que introduce en la red. En resumen, bajo este modelo, el hardware de red puede pasar a ser usado como un pool de recursos, optimizando así su uso y ganando en moldeabilidad en toda la red en su conjunto.

5.2.1.3 Aplicación actual y futura del concepto SDN

Aunque el concepto SDN se ha propuesto hace relativamente poco tiempo y está aún en el proceso de convertirse en una tecnología madura, hay ya muchas demostraciones de las posibilidades que ofrece. Y no sólo se trata de pruebas de concepto o prototipos, sino que ya hay aplicaciones en redes en producción.

El principal ámbito de aplicación de la SDN es hasta ahora el de los datacenters, donde se está aplicando el grado adicional de virtualización que ofrece para generar infraestructuras plenamente virtualizadas. La **virtualización de la red es el próximo paso natural en el objetivo de alcanzar un servicio de computación virtual y completamente interoperable**. Ya se han dado los primeros pasos en la virtualización de las redes a través de la construcción de modelos abstractos de los componentes más habituales de las redes actuales: links, routers, firewalls, balanceadores… **Con la SDN, la red se convierte en una entidad que se puede programar y controlar como cualquier otro elemento de la infraestructura de computación y que, por tanto, se puede virtualizar también.**

Un ejemplo de red SDN es Internet2, **la red estadounidense para investigación y educación** que está a punto de poner en marcha su red Ethernet a 100G basada en OpenFlow con el fin de probar servicios y aplicaciones de Big Data. **Deutsche Telecom**, por ejemplo, hace uso de OpenFlow para construir sus centros de datos, y destaca por haber propuesto y realizado la demostración de una arquitectura de red (Tera stream) en la que precisamente NFV y SDN son piezas esenciales. **British Telecom** contó sus pruebas con un BRAS software, en las que han obtenido muy buenos resultados desde el punto de vista de prestaciones, de calidad de servicio y de throughput. También presentaron las pruebas que han llevado a cabo con nodos CDN virtualizados. **Telefónica**, por su parte, participó en varias sesiones y mesas redondas, explicando sus líneas de innovación en este campo y aclarando las diferencias fundamentales entre el Cloud para IT y la virtualización para el ámbito de red.

6 ESTRUCTURA DE RED Y SERVICIOS DEL OPERADOR TELEFONICA

6.1 INTRODUCCIÓN

En este bloque del proyecto lo que pretendo analizar y dar a conocer es el **estado actual de las infraestructuras de red del operador Telefónica en España** así como los servicios ofertados sobre dichas redes.El sector de las telecomunicaciones está inmerso en un proceso de cambio muy significativo en el que la convergencia entre voz y datos y fijo y móvil. En el centro de este complejo proceso se encuentran las **redes IP de Nueva**

Generación (NGN). La actual situación de las nuevas tecnologías de la información y la comunicación está permitiendo que diferentes sectores como el de las telecomunicaciones, la radio o la televisión se fusionen en uno solo. Esta circunstancia, denominada **convergencia**, está cambiando la forma en que se comunican tanto las personas como los dispositivos.

Sin embargo, la actual tendencia de integrar todo tipo de servicios en una única infraestructura de red IP ha puesto de manifiesto las carencias **que tienen las soluciones IP clásicas**. Las redes IP tradicionales no están pensadas para transportar tráfico de voz, ya que este tráfico tiene unas características muy diferentes a los datos. Para solucionar estos problemas han aparecido en el mercado una gran cantidad de equipos, tecnologías y protocolos que, combinados de una manera adecuada, pueden permitir la realización de modelos de red que proporcionen, tanto al cliente corporativo como al cliente residencial, todo tipo de servicios multimedia. Estos son los modelos **de Red de Nueva Generación o Next Generation Networks (NGN), definida por Telefónica** como un modelo de arquitectura de redes de referencia que debe permitir desarrollar toda la gama de **servicios IP multimedia** de nueva generación como son las comunicaciones VoIP, videocomunicación, mensajerías integradas multimedia, integración con servicios IPTV, domótica…

El rápido crecimiento del tráfico en Internet y la paulatina migración hacia aplicaciones, a finales de la década de los 90 llevó a Telefónica de España a considerar que la red UNO de arquitectura compleja, baja capacidad de transporte y alta complejidad topológica, no satisfacía las demandas actuales y era necesaria la creación de una nueva red IP de nueva generación, altas prestaciones evolucionando la red UNO-IP/NURIA (NUeva Red Ip Avanzada) de Telefónica Data. Por esta razón, el operador finalizó, en octubre de 2001**, el despliegue de RIMA (Red Interactiva Multiservicio Abierta), una nueva red IP multiservicio** de última generación que incorpora elementos de routing de alta conmutación, capaz de integrar los nuevos perfiles de tráfico IP y multimedia, y de soportar, eficazmente, la creciente demanda de servicios de acceso a Internet, tanto en banda estrecha (accesos conmutados) como, y especialmente, en banda ancha (ADSL), así como otros servicios multimedia sobre IP y Redes Privadas Virtuales IP. La red RIMA ha sido diseñada, desplegada y habilitada para la prestación de servicios IP sobre cualquier tipo de acceso de cliente (Accesos por xDSL, RTC y accesos por líneas dedicadas punto-a-

punto o Ethernet) buscando la **escalabilidad** y la **calidad** como objetivos clave de diseño de la red. Esta red es una de las de mayor capacidad de las existentes en la actualidad en España y una de las más modernas de la UE. Actualmente cerca del 75% del tráfico de Telefónica transcurre a través de la tecnología IP.

Desde finales de 2007 se viene desarrollando un nuevo modelo de Red IP basado en la simplificación de las infraestructuras. En la situación de partida Telefónica disponía de **tres redes IP desarrolladas** verticalmente por cada una de las unidades organizativas **(Residencial (RIMA), Empresas (RUMBA (Red Unificada Multiservicio Banda Ancha)) y Móviles (RUD (Red Unificada Datos))** y un conjunto de redes de circuitos especializadas en los servicios de voz fija y móvil. Primero se fue unificando la integración del core de RUMBA en RIMA, y posteriormente la red de móviles RUD, buscando una **red mas compacta**, una **disminución de equipos** y una **arquitectura mas simple**.

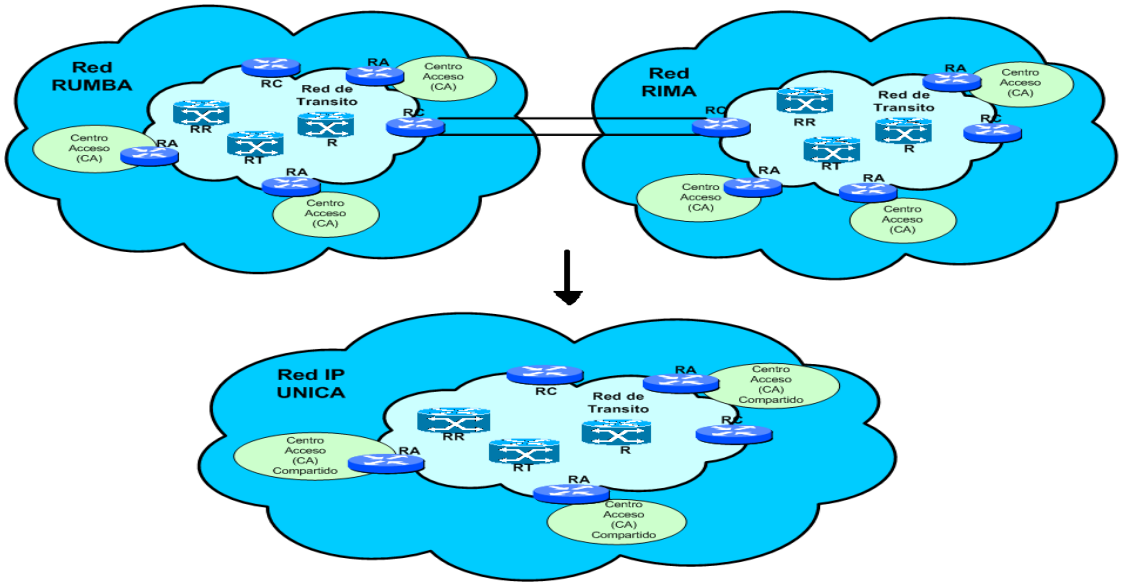


Figura 6.1.1 Integración redes de Residencial y Empresas. Elaboración propia.

En Marzo del 2009 se finaliza la integración de los nodos de acceso IP de la misma en el núcleo **IP/MPLS** común de la **Red IP Única**, eliminando por tanto **el core de la antigua red y convirtiendo dichos nodos de acceso IP en los centros de acceso IP** dedicados a los servicios orientados a las grandes empresas de Telefónica de España. Estos servicios están basados fundamentalmente en VPNs IP y conexión a Internet empleando accesos FR, ATM, xDSL, FTTH y Ethernet.

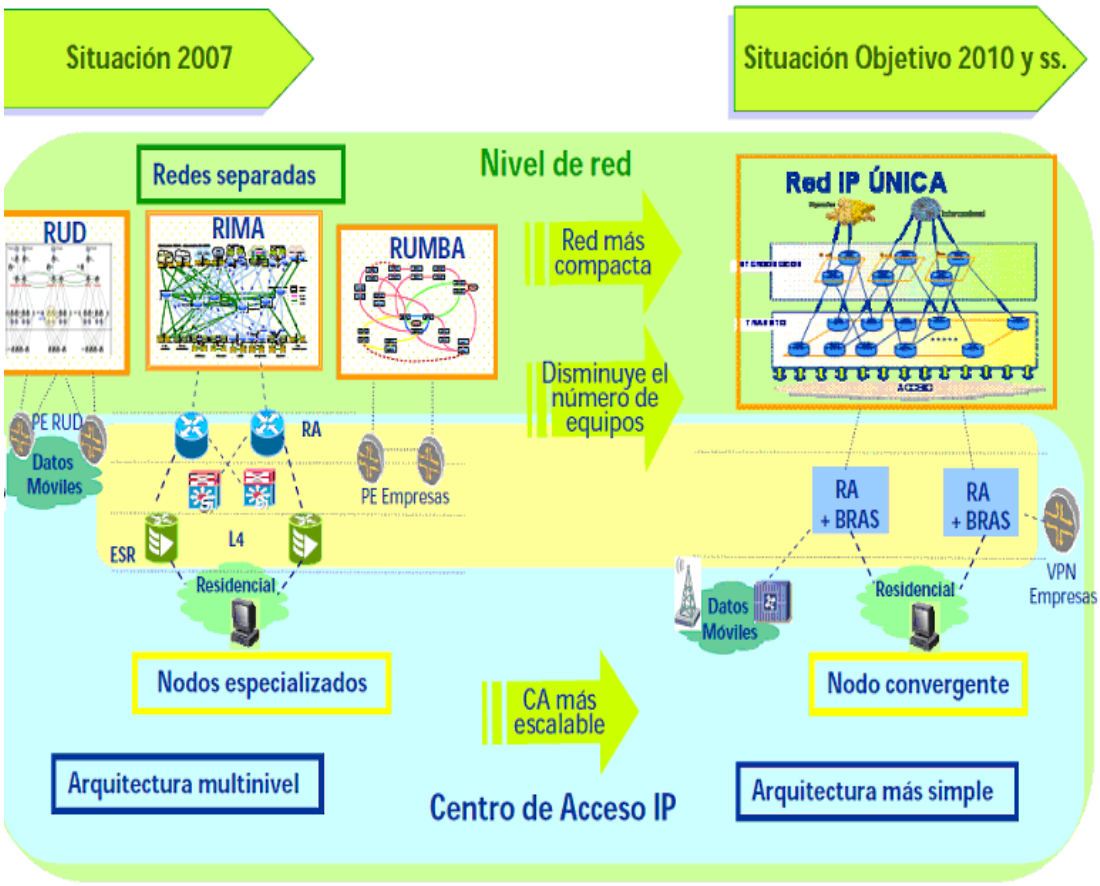


Figura 6.1.2 Evolución a modelo de red IP Única

Estas redes han ido evolucionando progresivamente en torno a arquitecturas NGN con transporte de flujos de voz y señalización sobre IP, para llegar al modelo de **Red IP Única** en el que actualmente nos encontramos. Este modelo está compuesto por:

1. **Una red (RIMA)** de altísima capacidad, disponibilidad, con tratamiento específico y diferenciado de los tráficos en función de su criticidad y abierto a Internet.
2. **Un anillo de conectividad crítica IP** de alta capacidad y con alta seguridad estructural, blindado al mundo Internet y dedicado a soportar el tráfico sensible (con requisitos de gran disponibilidad) y altamente crítico para el negocio.

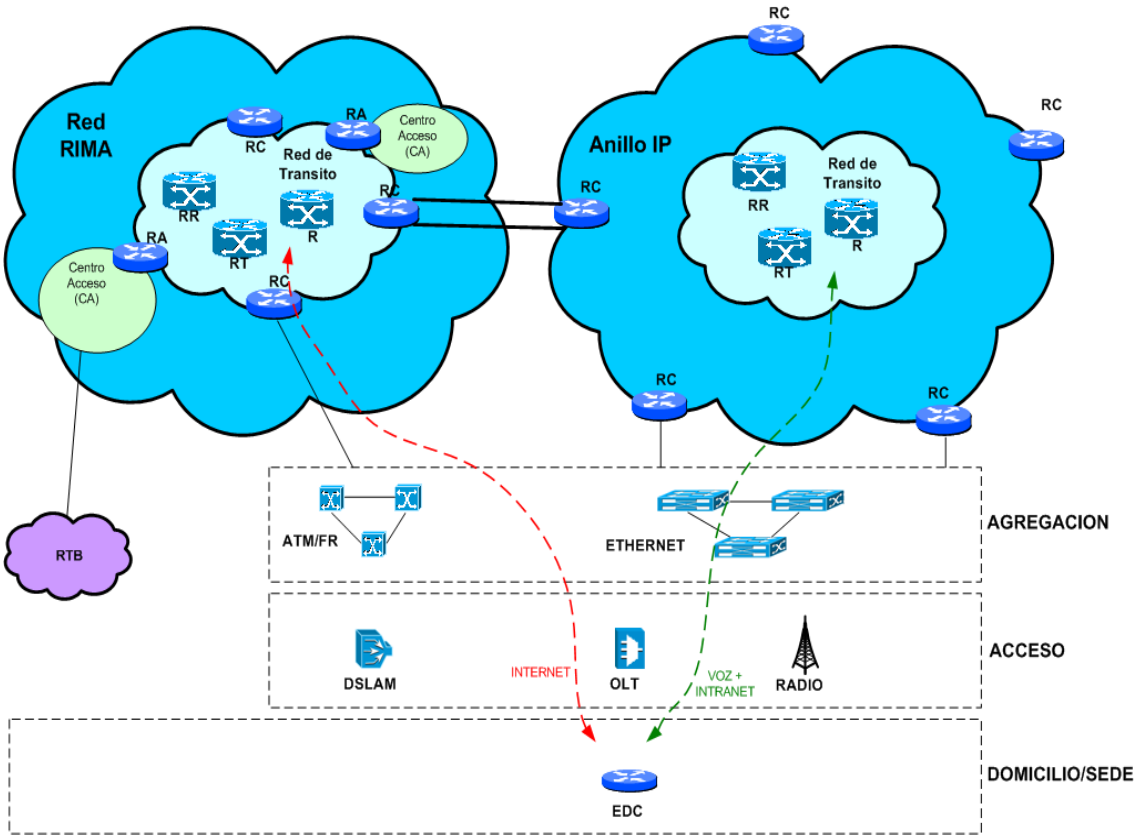


Figura 6.1.3 Composición de la red IP Única por RIMA y el anillo crítico. Elaboración propia.

La **aparición de nuevas tecnologías** de acceso (VDSL2, FTTH y Ethernet principalmente), y de nuevos servicios basados en las VPNs IP, ha supuesto un importante impulso para **evolucionar los nodos de acceso IP** dedicados a la prestación de los servicios a Empresas, tanto desde el punto de vista tecnológico (sustitución de eqquipamiento para introducir interfaces STM-64 y 10 GbE, etc), como en su diseño y cobertura.

6.2 ESTRUCTURA GENERAL DE LAS REDES DE TELEFONICA

La estructura actual de las redes de Telefónica de España viene representada en la figura siguiente:

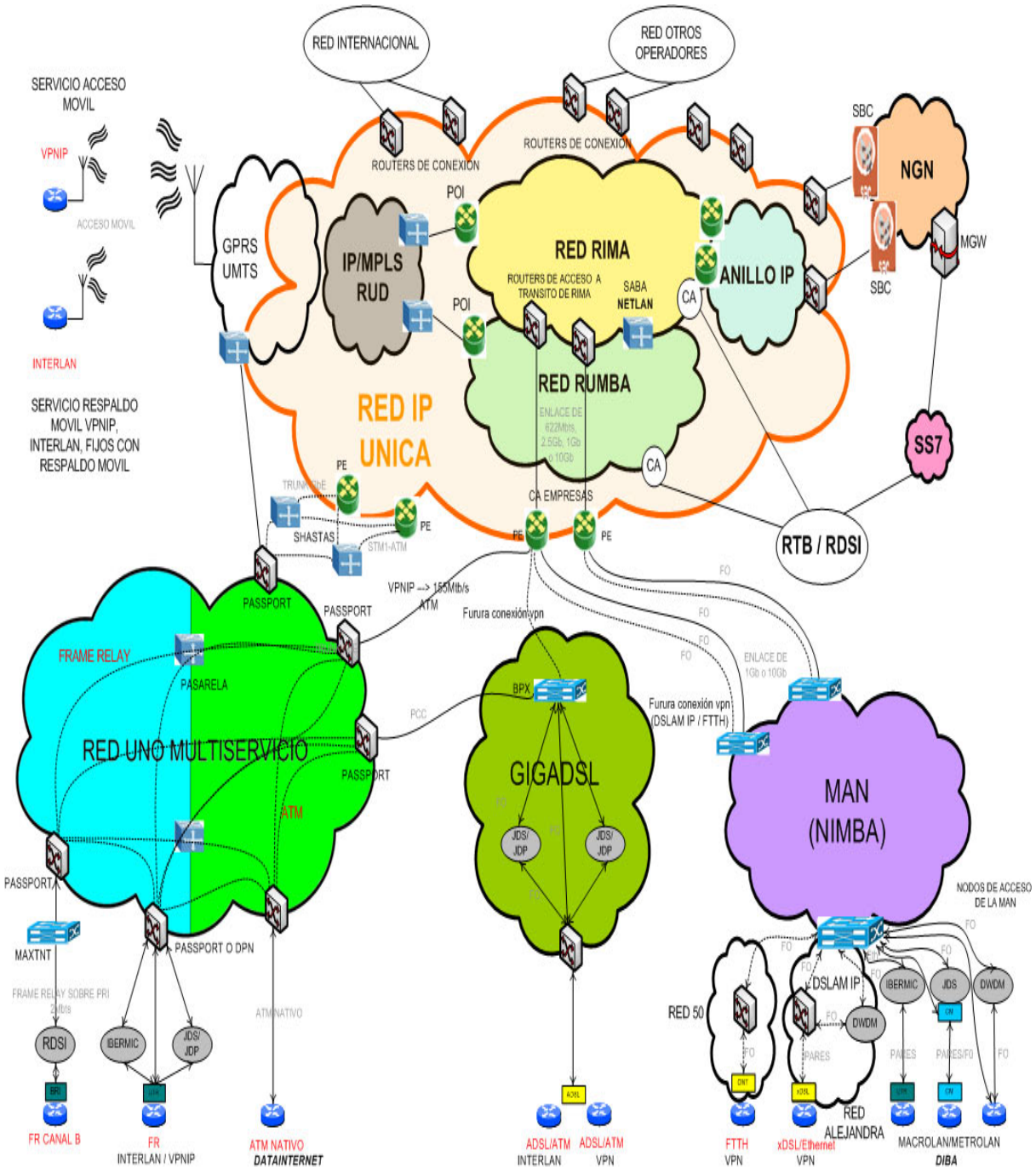


Figura 6.2.1 Estructura global de las redes de Telefonica de España. Elaboración propia.

Cada una de estas redes, así como sus servicios ofertados en la actualizar paso a detallarlos y analizarlos en los siguientes puntos del proyecto.

6.2.1 Red IP Única descripción general

La **Red IP Única** articula el conjunto de actividades de Telefónica España en torno a las redes e infraestructuras actuales y su evolución-transformación hacia una red única común. Su objetivo es el desarrollo y despliegue de una red única para **el soporte de los servicios multimedia convergentes fijo-móvil, cuyo transporte sea una red basada en "todo IP**" común con acceso de banda ancha, sobre cobre, fibra o radio. La Red IP Única **es una evolución de la red UNO-IP/NURIA de Telefónica Data**. Los **aspectos más relevantes** que llevo a Telefónica a plantearse una **evolución de la red UNO-IP a la Red IP Única** fueron:

- La red **UNO-IP su arquitectura era compleja y con dependencia de los recursos de transporte**, mientras **que al arquitectura en red IP se basa en tres niveles (acceso, transito e interconexión)** con elementos y rutas redundantes y equilibrado de carga con GigaRouters en el núcleo de red y con capas de gestión mas simple.
- La **red IP posee una alta capacidad de transporte** entre nodos mediante tecnología JDS (Jerarquía Digital Sincrona) y WDM (Wavelength-Division Multiplexing) y utilización de **protocolo MPLS** basado en el intercambio de etiquetas.
- En la red **UNO-IP la ingeniería de tráfico es difícil y costosa** mientras que en la **red IP única se emplean mecanismos de Clases de Servicio en los routers** y servidores de acceso RAS (Remote Access Server) y B-RAS (Broadband Remote Access Server).
- En la **red IP Única es fácil de implementar nuevas funcionalidades** ya que su arquitectura esta basada en productos comerciales, en UNO-IP son limitadas las nuevas funcionalidades.
- La red UNO-IP existía una falta de percepción de alta velocidad en el acceso a Internet con RTB o ADSL, mientras que con **red IP Única existe un mejor dimensionamiento de la red** y utilización de Caching en los Centros de Accesos (CA).
- La red UNO-IP su escalabilidad era muy limitada, mientras que la **red IP Única es una red pensada para crecer y con avanzadas capacidades**.

- La red **UNO-IP era limitada en capacidad de soporte de RPV (Redes Privadas Virtuales)**, poco escalable para servicios de streaming y difusión e ineficiente en gestión y consumos de direcciones IP. La red IP Única solventas todas las problemáticas anteriormente comentadas y además se basa en un modelo de acceso delegado sin túneles.

La Red IP Única el nivel de acceso está estructurado en zonas. Cada zona tiene un **Centro de Acceso (CA)**. Los usuarios pueden acceder a la red a través de la red conmutada (RTB o RDSI) o a través de accesos dedicados ADSL. Los Centros de Acceso realizan la **función de concentración de los usuarios**, tanto conmutados como permanentes.

Desde **la Red IP Única se tiene conectividad IP a redes externas** a través de los routers de conexión (RC) en el borde de la nube MPLS con las redes Internacionales y redes con otros operadores de red de España (Vodafone,Orange….). Además, posee conectividad con la red NGN (New Generation Network) a través de los SBC (Session Border Controller) que actúa de elemento frontera y que interactúa con las centralitas IP de los clientes mediante de la Red IP Única.

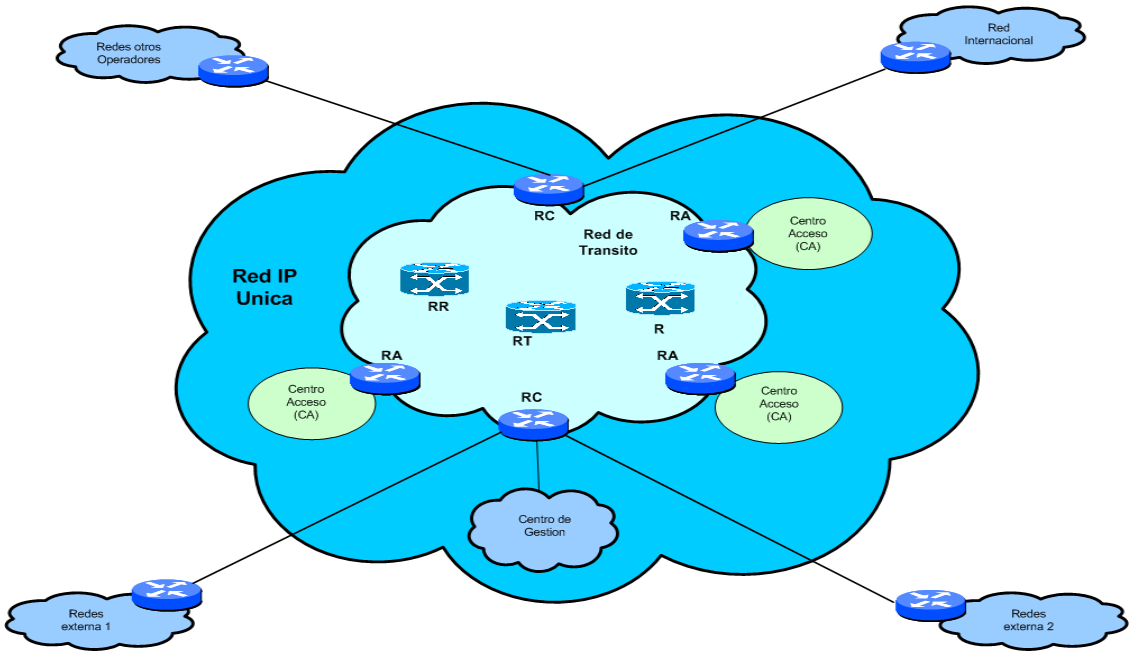


Figura 6.2.2 Redes que interconectan con la red IP Única.Elaboración propia.

Con **la red UNO o multiservicio de nivel dos se tienen conectividad mediante los SHASTAS para ofrecer los accesos Frame-Relay o ATM nativo a la red IP**. Para accesos ADSL se ofertan a través de la Red GigADSL que tiene conectividad con la red multiservicio o directa con los centros de acceso de la red IP.

La conectividad a nivel metropolitano/provincial se sustenta en la infraestructura asociada a la MAN. Son las redes MAN (Metropolitan Area Network) la cual suele haber una o mas por provincia en dependiendo de volumen de trafico a soportar. Dicha **infraestructura de nivel 2 basado en switches**, proporciona tanto la conectividad entre sedes del cliente en la misma área provincial como la conectividad con los routers de conexión de la red IP Única para proveer las comunicaciones interprovinciales.

Como he comentado anteriormente la **Red IP Única esta formada por la unificación de la red RIMA, red RUMBA, red RUD y el anillo critico** para trafico priorizado y de alta criticidad para conseguir una arquitectura de red mas simple y eficaz.

6.2.2 Red UNO (Multiservicio) descripción general

La **red Uno** o multiservicio es la **evolución de la red Iberpac** que se comento anteriormente en el proyecto. La red **se basa en tecnología ATM y Frame-Relay** empleando equipos Passport de Nortel para realizar la **conmutación de nivel 2** de las tramas. En el backbone de la red los equipos tienen una capacidad transmisión de hasta 2,5 Gb. Para el acceso a la red y concertación de servicios X.* también se emplean equipos DPN.

La red ofrece conectividad multiprotocolo. Los **accesos** de los clientes pueden ser **ATM, Frame-Relay, Ethernet**, y también otros protocolos como **X.25, X.28 y X.32**. La red también sirve de acceso a clientes que conectan a la red IP Única.

Permite **conexiones permanentes (CVP) y conmutadas (CVC) extremo a extremo** con utilización de direccionamiento IP público o privado, o de protocolos distintos de IP. Se basa en la **creación de redes privadas virtuales con una infraestructura compartida por clientes** manteniendo las mismas prestaciones que si fuera una red privada, reduciendo

costes y aumentando rendimiento. Sobre la red se permiten diferentes servicios, unos a extinguirse y otros todavía comercializable que se explicara mas adelante en el proyecto.

6.2.3 Red NGN / IMS descripción general

La **red NGN** de Telefonica se fundamenta en la arquitectura NGN (Next Generation Network) y en una **estructura de control** alineada con las **especificaciones resultantes del 3GPP** (Third Generation Partnership Project). **Su arquitectura se basa en un modelo IMS** el cual **separa en niveles** la funcionalidad de las soluciones extremo a extremo (end-to-end): **Aplicaciones, Control, y Conectividad**. De esta forma permite a cada nivel desarrollarse y evolucionar de forma independiente al resto, estando unos niveles condicionados más que otros, por el mercado y la evolución de la tecnología, como puede ser el caso de la migración en el nivel de conectividad a nuevas tecnologías de transmisión sin necesidad de que el resto de los niveles se vean afectados.

Aunque la solución tiene por objetivo el ofrecer una amplia oferta de servicios de voz y en un futuro aplicaciones multimedia, permiten la interconexión con redes de circuitos tradicionales (RTC), PSTN mediante Gateways y con la Red IP Única mediante los SBC. Mas adelante en el proyecto explicaré detalladamente el funcionamiento y servicios ofertados sobre la NGN.

6.2.4 Redes MAN NIMBA

Las **redes NIMBA (Nuevas Infraestructuras Metropolitanas de Banda Ancha)** son infraestructuras diseñadas para proporcionar **conectividad de banda ancha** basadas en el **trasporte de tráfico Ethernet** entre redes de área local de los clientes ubicadas en lugares diferentes de la **misma provincia o con los routers de acceso de la red IP Única** para las comunicaciones interprovinciales.

6.2.4.1 Arquitectura de red

La estructura que tendría una MAN se basaría en la siguiente figura:

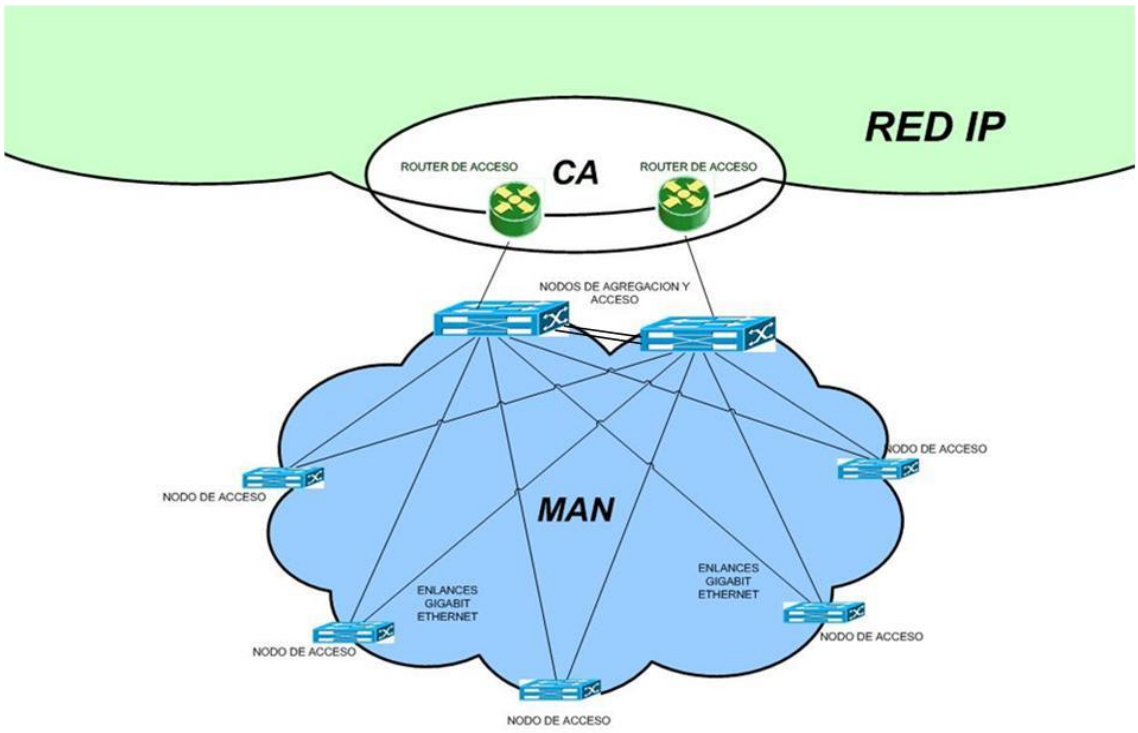


Figura 6.2.3 Arquitectura genérica de una red MAN. .Elaboración propia.

Se trata de una **red multipunto dividida en dos niveles, de acceso y agregación** .En el nivel de **agregación** esta formado por dos o mas nodos de agregación que permiten la **conectividad con la red IP Única mediante los Routers de Acceso** que forman parte de los CA y agrupan los enlaces GigabitEthernet de los nodos de acceso de la MAN a los que se conectan los clientes. Cada nodo de **acceso esta dotado de al menos dos enlaces GigabitEthernet para dar redundancia** a las conexiones en caso de caída de una de ellas y cada ruta óptica no es coincidente. Además por seguridad también son redundantes los nodos de accesos (1+1). Los **enlaces GigabitEthernet son de tipo óptico** (802.3z) de fibra monomodo (1000BASE-LX) para distancias de hasta 10 km, y de tipo 1000BASE-LH/ZX para mayores distancias, aproximadamente de hasta 40 km. De precisarse mayores alcances, se recurre a sistemas de transmisión JDS, WDM, etc.

Los nodos, son conmutadores son switches Ethernet de tipo carrier-class, es decir con matriz y módulo de control redundante que **trabajan a nivel dos**, es decir, a nivel de enlace del Modelo OSI. Ofrecen **conexiones multipunto Ethernet** que son un recurso lógico que se establece en la MAN para ofrecer conectividad entre una serie de accesos.

Una conexión multipunto Ethernet funciona como un circuito virtual multipunto de forma **simular a una red de área local (LAN) tradicional** que transporta transparentemente tramas Ethernet de los diversos equipos que se conectan a la misma.En la red MAN además **se ofrecen diferentes calidades de servicio** para priorizar el tráfico en función de la criticidad y sensibilidad del tráfico a transportar. La prioridad viene marcada con 3 bits en la trama que inserta el cliente en la red **según el estándar 802.1p**. Adicionalmente como la MAN es vista como una red LAN grande con accesos diversificados, **emplea mecanismos para evitar tormentas** de broadcast y una topología libre de bucles. El protocolo **Rapid Spanning Tree (IEEE 802.1d)** bloquea los caminos redundantes para evitar bucles.En los **accesos** a la MAN, se utiliza **multiplexación** de conexiones sobre un mismo puerto físico según el protocolo **802.1Q.** Según terminología de dicho protocolo, **cada conexión multipunto Ethernet se materializa en una VLAN y queda identificada en dicho acceso mediante un identificador de VLAN** para conseguir independencia entre el trafico de los diferentes clientes.

6.2.4.2 Tecnologías de multiplexación de tráfico

Para garantizar el aislamiento en la MAN del trafico de los clientes se emplean dos tecnologías**: VPLS o IEEE 802.1Q**. **Para más información sobre el protocolo VPLS y el 802.1Q consultar el documento memoria_anex.pdf apartado ANEXO4.**

6.2.4.3 Tipos de accesos a la red MAN

Los accesos a la red MAN pueden ser por fibra, xdsl o GPON (Gigabit-capable Passive Optical Network) **y cobre**. **Para información mas detallada de los tipos de acceso a la MAN consultar el documento memoria_anex.pdf apartado ANEXO5.**

Para esta última modalidad Telefónica define el acceso Cobrelan que ofrece ofrecen un punto de acceso a la MAN con las siguientes características:

- Acceso Ethernet de 10 Mbps.
- Modo transmisión full duplex.
- Interfaz 10BaseT según 802.3 para cable UTP categoría 3 o superior con conector RJ45.

Para obtener información sobre los equipamientos empleados en los accesos a la red MAN como son las UTRs, los CdM y los ONT consultar el documento memoria_anex.pdf apartado ANEXO6.

6.2.5 Redes de acceso para líneas fijas con arquitectura XDSL, FTTH

Las redes **de Acceso de Banda Ancha de Telefónica de España** para líneas fijas basadas en tecnología XDSL y FTTH presentan **3 arquitecturas diferenciadas** bajo el nombre de tres redes: **GigADSL, Alejandra y Red 50.**

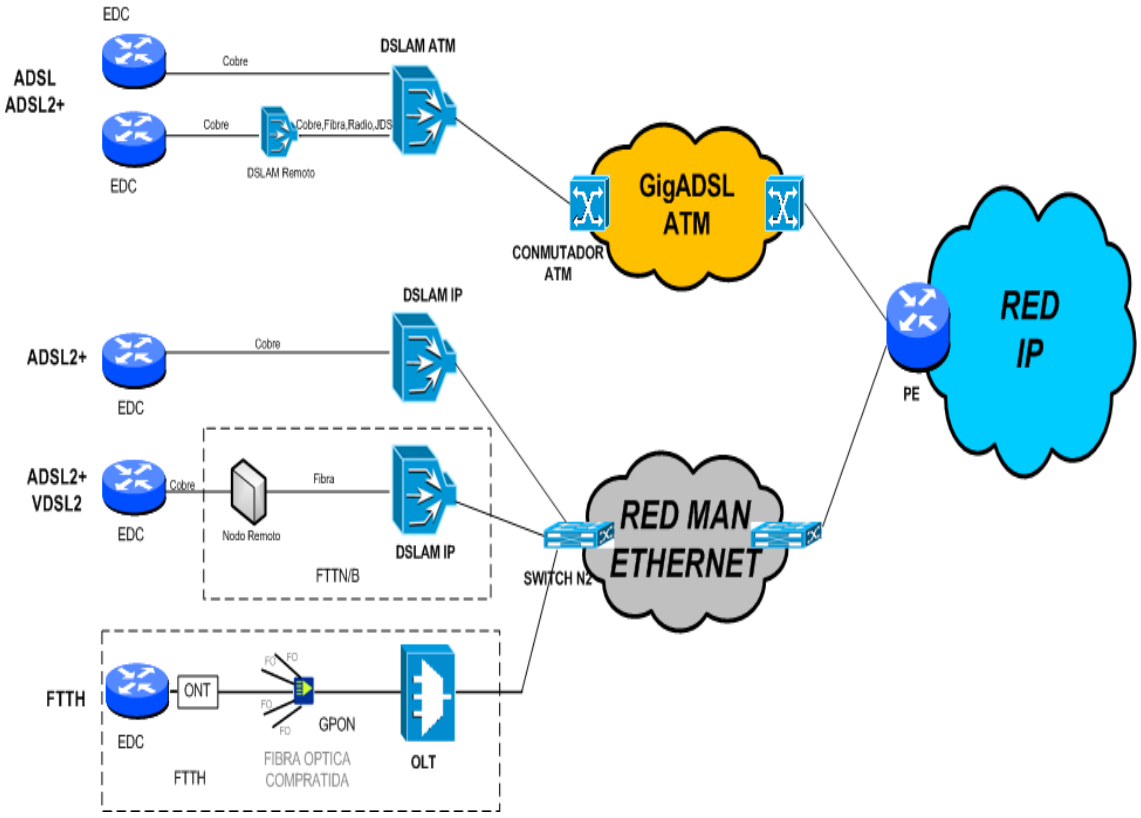


Figura 6.2.4 Arquitectura actual de red de acceso fijo. Elaboración propia.

6.2.5.1 GigADSL

La **red GigADSL es un servicio de nivel 2**, para bucles de abonado indirectos basado en el **establecimiento de un PVC ATM** entre el usuario y **el PAI (Punto de Acceso**

Indirecto) local del operador que contrate el servicio. Se trata de un servicio local cuyo tráfico está designado a una demarcación.

6.2.5.1.1 Descripción técnica de la arquitectura de la red

El **acceso se compone de un bucle de abonado de par de cobre** basado el **tecnología ADSL** (hasta 8Mbps) **o ADSL2+** (hasta 20Mbps) con un modem en el domicilio del **cliente ATU-R y otro en central ATU-C** que pueden ser un **DSLAM o MUXFIN que multiplexan las conexiones** ADSL/ADSL2+ que reciben. El sistema de transporte proporciona al DSLAM una interfaz de transmisión hacia el backbone de tipo STM-1 o E3. El **backbone se compone de un tramo ATM** hasta un **punto de interconexión,** donde se concentran todos los accesos de una determinada zona geográfica. Este **punto de interconexión o PCC** es recibido en un **Passport de la Red Multiservicio** que hace las funciones de red de agregación donde los PVC de ATM se encaminarán hacia el router de acceso de la Red IP Única pertenecientes a los CA. **Sobre este PVC de ATM se encapsula directamente el protocolo IP** (IPoATM). **El PCC también sirve como punto de interconexión con otros operadores.** Estos accesos tendrán características propias fijadas por la definición del servicio GigaADSL como son, caudales asimétricos y parámetros SCR y PCR de ATM específica.

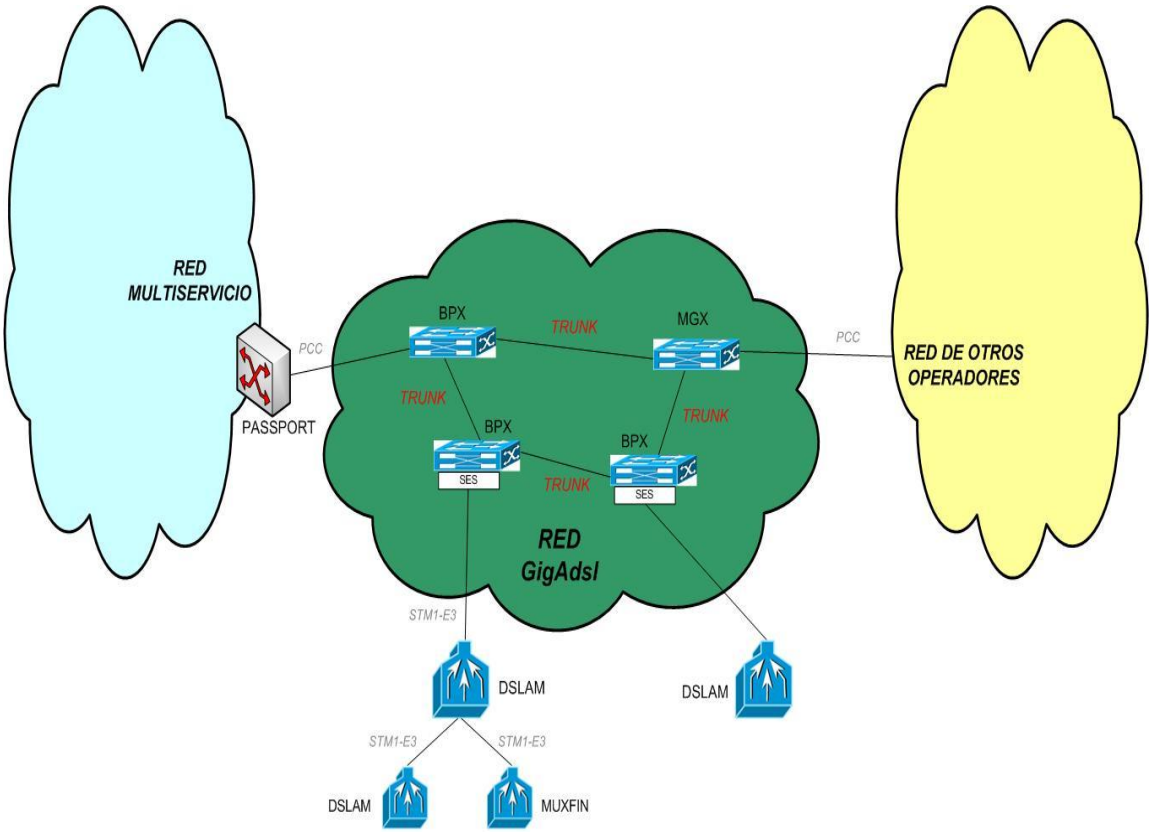


Figura 6.2.5 Esquema de conectividad de red GigADSL. Elaboración propia.

6.2.5.1.2 Equipos que conforman la red GigADSL

Los equipos que intervienen en la red GigADSL tal y como muestra la figura anterior son **los DSLAM, los MUXFIN, los BPX, los MGX y los SES**. Para obtener una información de las características de cada uno de ellos consultar **el documento memoria_anex.pdf apartado ANEXO7.**

6.2.5.1.3 Señalización en el núcleo de la red

En la GigADSL **coexisten 2 tipos de protocolo de señalización y encaminamiento**:

- **AutoRoute (AR)**
- **PNNI**

Para más información sobre los protocolos AR y PNNI consultar el documento memoria_anex.pdf apartado ANEXO8.

6.2.5.2 Red Alejandra

La red Alejandra esta **basada una arquitectura Ethernet** pensada para ofrecer servicios de VoIP, TV e Internet **donde la red GigADSL no dispone** de los mecanismos para soportar estos servicios. Básicamente la red Alejandra está **pensada para el servicio Imagenio de Telefonica sobre accesos con tecnología ADSL2+ y VDSL2** sobre par de cobre que se multiplexan en DSLAM IP.

6.2.5.2.1 Descripción técnica de la arquitectura de la red

Tal y como he comentado anteriormente el **acceso a la red Alejandra se emplea tecnología ADSL2+ y VDSL2** ya que con esta tecnología se permite mayores anchos de banda que el ADSL2+ a distancias inferiores a 1 km para ofrecer con calidad los servicios de Imagenio. **El DSLAM pasa de ser un conmutador ATM a comportarse como un conmutador Ethernet** entre dos medios físicos diferentes (xDSL en el acceso del usuario y Gigabit Ethernet hacia el lado de la red). Los DSLAMs de este tipo reciben el nombre de **DSLAMs IP**.

Se definen dos PVCs de acceso para el acceso de los usuarios de ADSL2+, uno de ellos dedicado a todos los servicios **asociados a la TV** y otro compartido entre el **tráfico de Internet y el de VoIP**. Al compartir Voz e Internet **el mismo PVC se aplicará mecanismos de calidad de servicio QoS** en el router para **priorizar el tráfico de Voz** frente al de datos en caso de congestión en sentido subida , que es donde hay un ancho de banda menor y es un punto donde se puede dar la congestión fácilmente. En el resto de la red no se aplica QoS ya que se estima que está sobredimensionada y no se va a producir congestión.

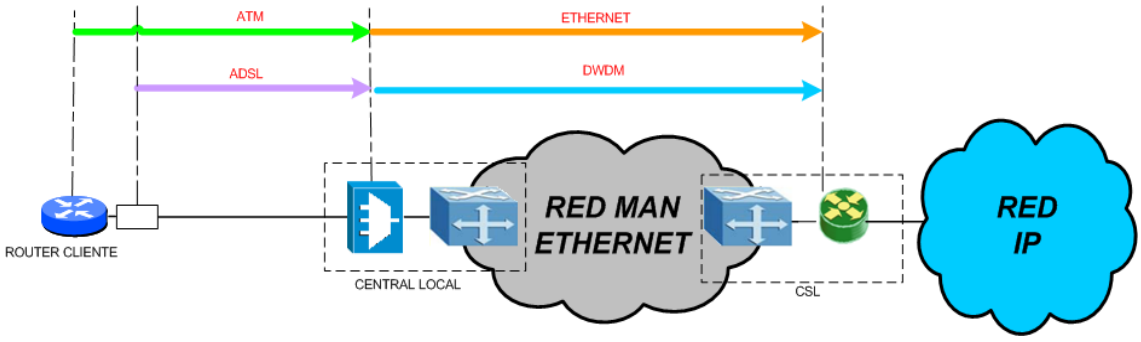


Figura 6.2.6 Esquema de conectividad con la red Alejandra. Elaboración propia.

Los **diferentes tipos de tráficos que confluyen hacia la red MAN** (Multicast y Unicast) son agregados por servicios sobre **VLANs diferenciadas desde los** DSLAM IP utilizando VLAN stacking hasta los correspondientes centros de servicio.

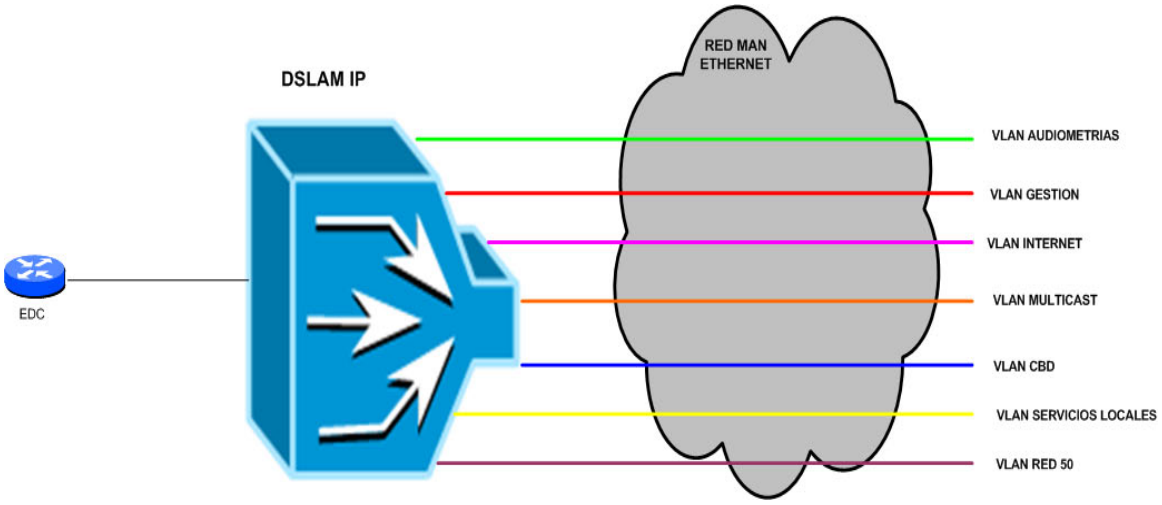


Figura 6.2.7 Esquema de vlanes stacking por servicio en DSLAM IP Alejandra.Elaboración propia.

La **conexión troncal que une los DSLAM IP a la red Ethernet se comparte entre todos los servicios** que se prestan desde ese equipo. Cada uno de estos servicios tiene sus propias necesidades en cuanto a las conexiones que necesita establecer a través de la red de agregación, y cada una de **estas conexiones debe ser identificada con una etiqueta de VLAN 802.1Q**, ya que basándose en esta etiqueta la red Ethernet aplicará a cada conexión el tratamiento deseado. Un puerto de conexión del PE de la Red IP Única a la red Ethernet recibirá interconexiones de varios DSLAM IP, por lo que será necesario que las etiquetas **de VLAN en este lado sean diferentes para cada concentrador**. Gracias a la **capacidad que ofrece VPLS de desacoplar las etiquetas** en cada uno de los extremos de la conexión, esto es posible.

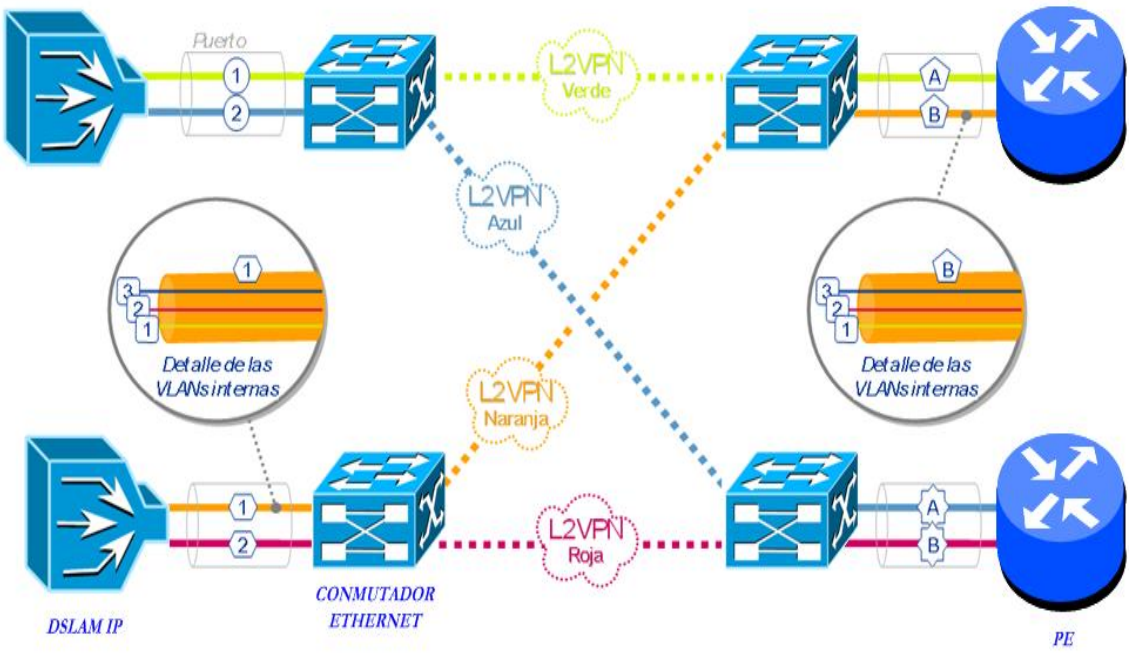


Figura 6.2.8 Esquema de vlanes en nodos de la MAN con tecnología VPLS.Elaboración propia.

Para saber los tipos de conexiones con la red Alejandra y las interacciones entre las capas de protocolos, consultar el documento memoria_anex.pdf apartado ANEXO9.

6.2.5.3 Red 50

La Red 50 es un proyecto estratégico de renovación de la red de acceso para las ciudades más importantes, cuyo objetivo es aumentar la cobertura de la red de acceso **ofreciendo capacidades de hasta 100 Mbps** al 60% de hogares españoles para poder ofrecer los servicios de Imagino con calidad. La **tecnología empleada se basará en acercar la fibra óptica (FO)** al usuario. El radio de cobertura desde el nodo para velocidades de 100Mps es de hasta 600m, reduciéndose a 300m con conformado espectral (cuando hay que evitar interferencias sobre señales procedentes desde la central local = ULL). Existen por tanto dos escenarios de fibra óptica que son FTTH y FTTB. **Para saber en que consisten los dos escenarios de fibra óptica, consultar el documento memoria_anex.pdf apartado ANEXO10.**

6.2.5.3.1 Elementos que componen una red FTTH/FTTB

Los elementos que componen una red FTTH/FTTB **son el OLT, el ONU/ONT, el Splinter y el MDU. La explicación de cada uno de estos elementos se puede connsultar en el documento memoria_anex.pdf apartado ANEXO11.**

6.2.5.3.2 Descripción técnica de la arquitectura de la red 50

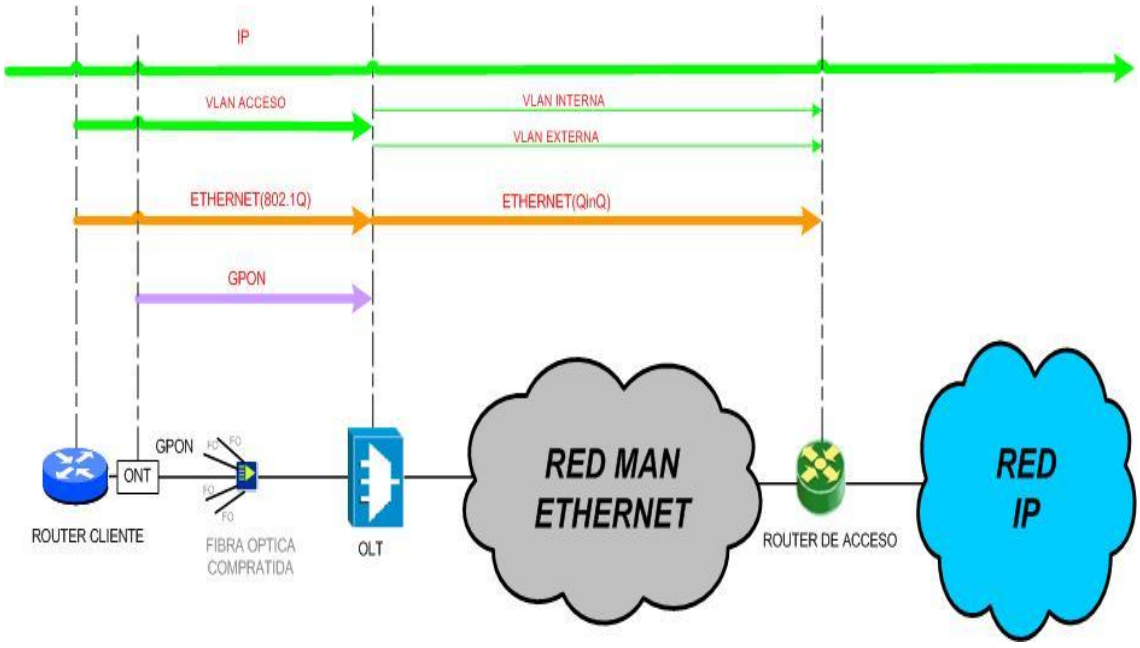


Figura 6.2.9 Pila de protocolos para accesos FTTH sobre la red 50.Elaboración propia.

Aunque existen varias tecnologías de transporte que funcionan sobre FTTH/FTTB, **la red 50 emplea GPON. La explicación mas detallada sobre la tecnología GPON se puede consultar en el documento memoria_anex.pdf apartado ANEXO12.**

6.2.5.3.2.1 Interacciones en la capa GPON

En la capa GPON se seguirán los criterios de funcionamiento definidos par el resto de servicios ya implementados sobre esta tecnología. **Se asignará en la PON un puerto GEM** (usado en sentido ascendente y descendente**) y un T-CONT (usado sólo en sentido ascendente) para cada conexión. Sobre cada puerto GEM se transportará una única VLAN Ethernet**.

A diferencia de los pares metálicos, la red óptica pasiva entre las ONT y la OLT **es un medio compartido** y por tanto puede existir congestión. Así que en este caso sí tiene sentido que **exista a este nivel una garantía de caudal** diferenciada entre los accesos residenciales y los accesos de Grandes Clientes. Además, la tecnología GPON permite esta garantía diferenciada. Por tanto, los accesos destinados al servicio VPN IP tendrán una **garantía de caudal (CIR) en la red de acceso GPON del 50%**.

6.2.5.3.2.2 Interacciones en la capa Ethernet

Una **ONT se conecta con los equipos de cliente** a los que presta servicio mediante **puertos Ethernet**. Dentro de esta red Ethernet "local", **cada VLAN indica un "servicio" diferente**, de manera que en función de la VLAN por la que se cursa un tráfico determinado, la ONT aplica un tratamiento distinto, según lo especificado para cada servicio.

Por tanto, el valor de esta etiqueta de VLAN usada en el enlace router-ONT debe ser diferente del utilizado por otros servicios, conexiones o instancias del mismo servicio sobre esa misma ONT, ya que es el medio de distinguir entre ellos. Desde el punto de vista de un router, este valor podría repetirse en otros enlaces router-ONT del mismo árbol PON mientras que las ONTs y la OLT sean capaces de individualizar cada conexión.

La **OLT prolongará estas VLANs Ethernet** que se establecen desde **el router hasta el RA de la red IP Unica a través de la red de agregación Ethernet MAN**. Puesto que los routers están conectados a la ONT a través de una conexión Ethernet "real", no presentan problemas a la hora de manejar las etiquetas 802.1q y las marcas de prioridad que sí se dan en tecnologías como ADSL2+/IP.

Al igual que en VDSL2, **la OLT progresará de manera transparente las prioridades 802.1Q de las tramas que reciba**. En sentido ascendente (router→OLT), deberá reflejar sin cambios la prioridad recibida del router en la cabecera externa 802.1Q que añade. En sentido descendente (OLT→router), se recomienda en la medida de lo posible mantener el marcado que se ha recibido.

6.2.5.3.2.3 Interacciones en la capa IP

No existe ninguna interacción a nivel IP entre el router y la ONT o la OLT en los accesos GPON.

6.2.6 Redes de acceso para líneas móviles

En el apartado 11.1.5 explicaba las diferentes redes de acceso para tecnología fija como eran las redes GigADSL, Alejandra y Red 50. Para el **acceso a la Red IP Única basado en tecnologías móviles se emplean las redes GSM, GPRS, UMTS y la nueva LTE**. La arquitectura actual de las redes GSM/UMTS estaría representado en el siguiente esquema:

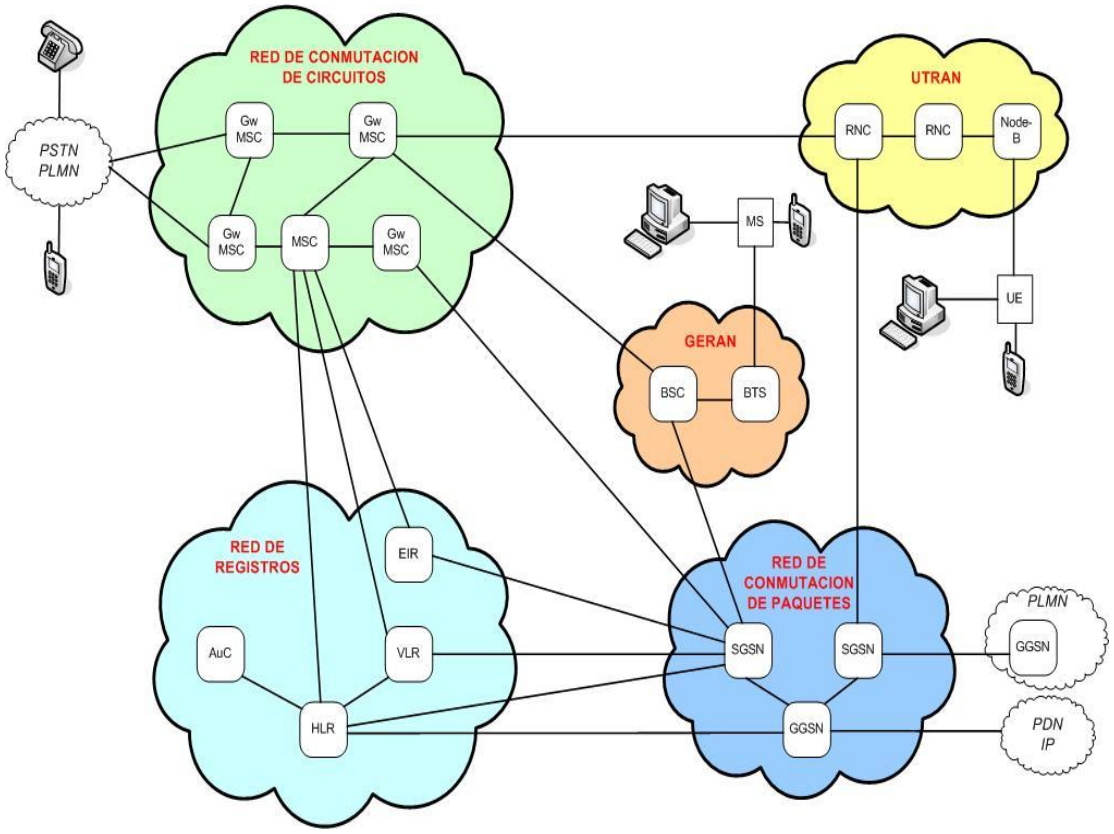


Figura 6.2.10 Esquema de la arquitectura de redes GSM/GPRS/UMTS. Elaboración propia.

Para obtener una información detallada de la arquitectura de las red GSM/GPRS y UMTS **connsultar en el documento memoria_anex.pdf apartado ANEXO13.**

6.2.7 Redes de transporte para el tráfico de las redes móviles GSM/UMTS

Hasta **mediados del año 2009**, para el transporte de tráfico e interconexión de **las redes GSM/UMTS** formada por los elementos descritos anteriormente, **se apoyaba era una red con tecnología ATM específica desplegada al efecto y con cobertura geográfica nacional**, el transporte se daba por medio de circuitos dedicados E1´s sobre la Red de Transporte Multiservicio SDH de Telefónica.

A **partir del 2009**, debido a la mejor relación velocidad/precio y escalabilidad proporcionada por los interfaces Ethernet/IP frente a ATM, la tendencia actual es migrar los servicios basados en tecnologías **tradicionales a tecnología Ethernet/IP consiguiendo una "Banda Extensa Móvil"**. Por tanto, en la actualidad la **conectividad de las redes móviles** se sustenta en **dos tecnologías de agregación** bien diferenciadas:

1. Red **ATM** de Servicios Móviles.

2. Red **Ethernet Multiservicio MAN** de cada provincia.

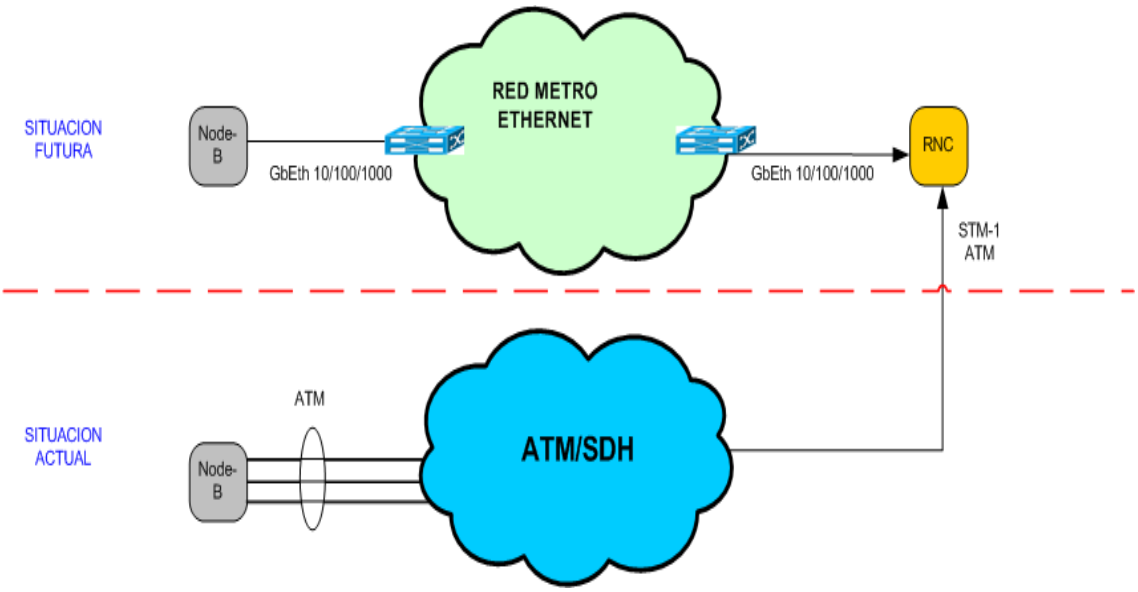


Figura 6.2.11 Esquema de redes de transporte para el tráfico móvil. Elaboración propia.

Ambas redes **proporcionan conectividad con la Red IP Única**, a través de los **centros de accesos (CA) de la red RUD que ya está integrada de forma global en la red IP**, para ofrecer los servicios correspondientes tal y como muestra el siguiente esquema.

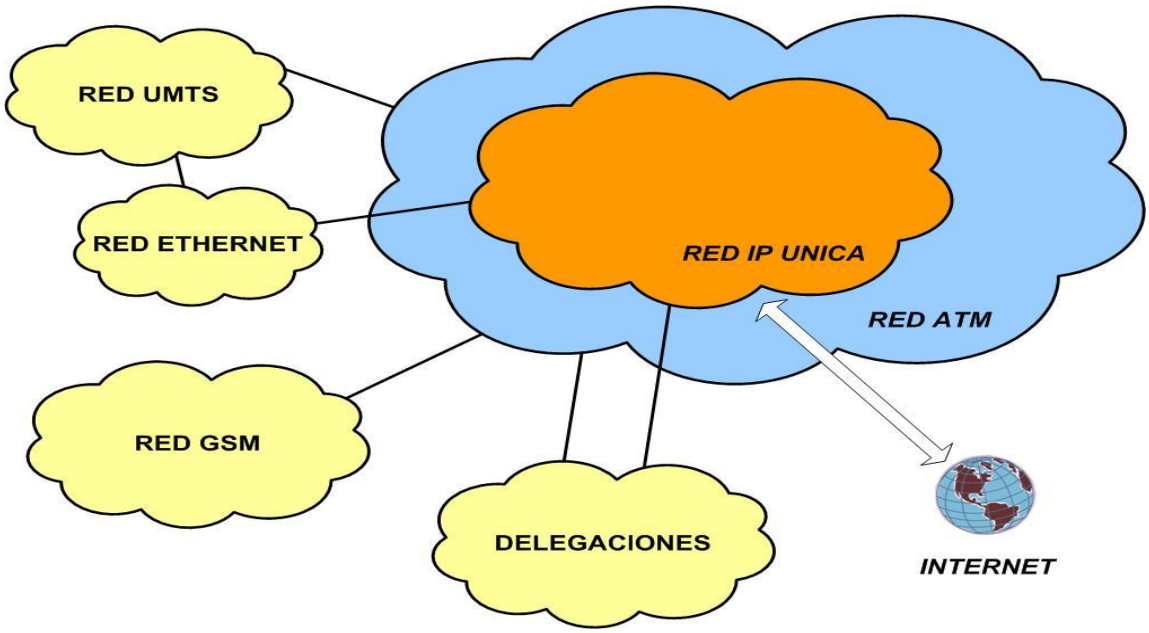


Figura 6.2.12 Esquema de conexión de la red Ethernet MAN Y ATM con la red IP Única. Elaboración propia.

6.2.7.1 Transporte empleando la red ATM

La red ATM proporciona el **transporte de parte de los flujos de tráfico GSM y UMTS**. Dichos flujos, de forma resumida, son **información entre diferentes elementos de las redes GSM y UMTS**. De los múltiples flujos de tráfico cursados a través de la red ATM, el crecimiento mayor se espera en el tráfico de datos UMTS. Actualmente menos del 20% del tráfico entre nodo B-RNC se cursa por la red ATM. El **porcentaje de dicho tráfico UMTS cursado por la red ATM tenderá a cero en los próximos años**, siendo dependiente el descenso del tráfico **cursado de soluciones Ethernet/IP** alternativas.

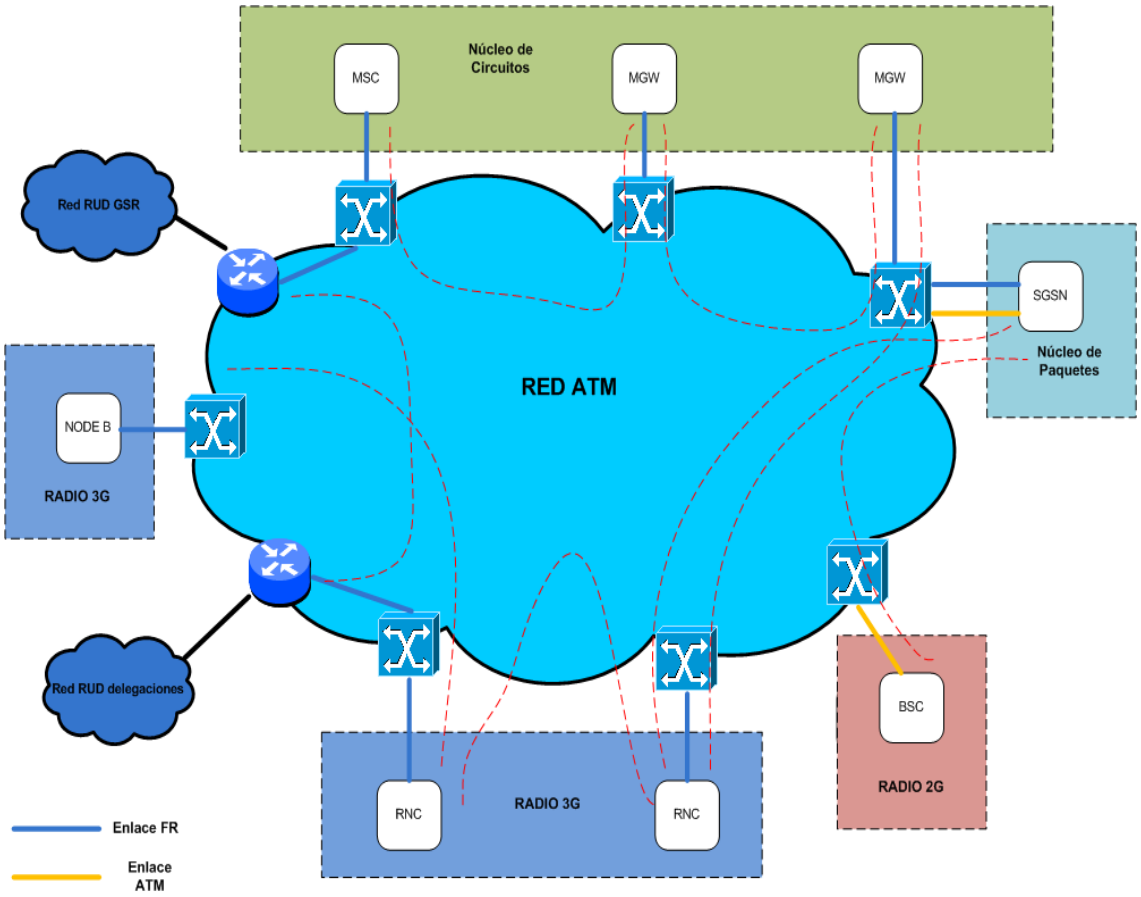


Figura 6.2.13 Flujos de tráfico de servicios móviles cursados por la red ATM. Elaboración propia.

Además de realizar la función de transporte del tráfico UMTS entre equipos de radio y equipos de núcleo, la red **ATM también se encarga de transportar flujos entre routers de la red IP Única mediante VCC de ATM**.

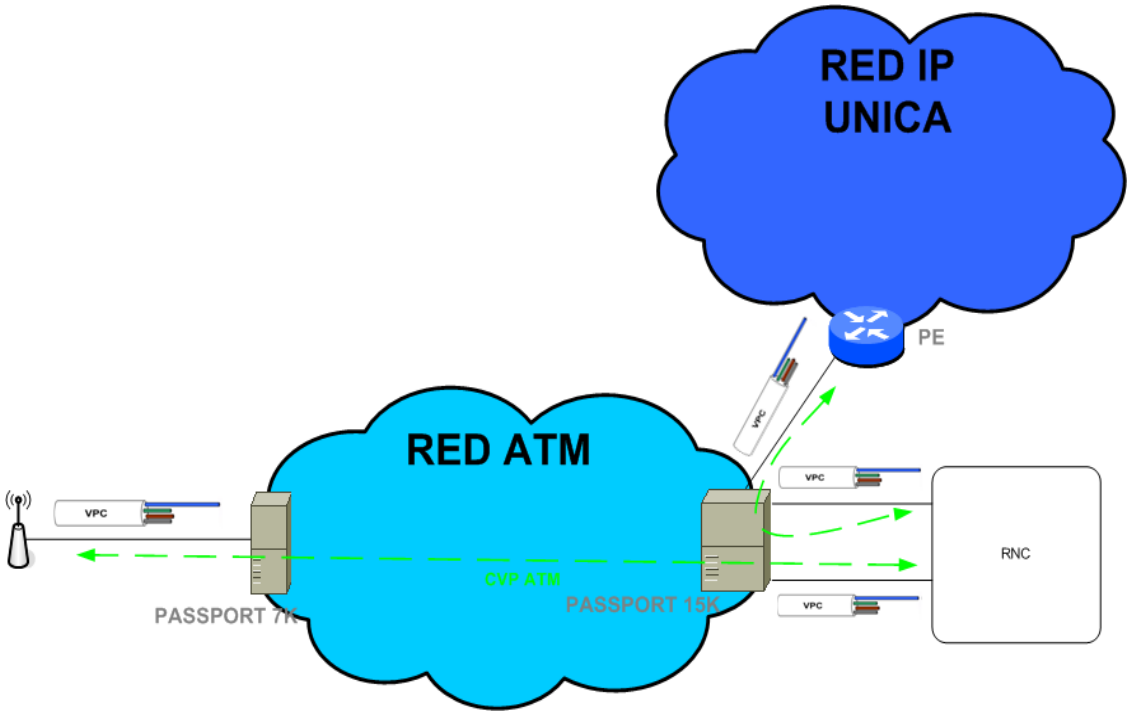


Figura 6.2.14 Flujos de tráfico con routers de la red IP Única mediante VCC ATM.Elaboración propia.

Hasta el 2009 la red ATM proporcionaba de forma exclusiva la conectividad entre los elementos de radio UMTS (nodo B - RNC), entre equipos de radio y núcleo de circuitos (RNC-MGW) y paquetes (RNC-SGSN). A lo largo de estos años se han realizado migraciones de flujos de tráfico a redes Ethernet/IP, con el fin de proporcionar servicios de banda ancha móvil.

7.2.7.1.1 Descripción de la arquitectura de la red ATM

La Red ATM **es una red monovendedor formada por equipos de Ericsson** basada en la tecnología ATM para el transporte de tráfico. La **red ATM se divide en tres niveles topológicos**:

- **Backbone: formado por los equipos PP15K**, que además de las **funciones de acceso/agregación** componen la malla de backbone.
- **Acceso/agregación**: compuesto por todos los PP15K, encargado **de proporcionar el acceso de los equipos de radio y núcleo**, así como realizar la agregación de dicho tráfico.

- **Acceso: formado por equipos PP7K**, proporcionan el **acceso a determinados elementos de radio: BSC's y Nodos B.**

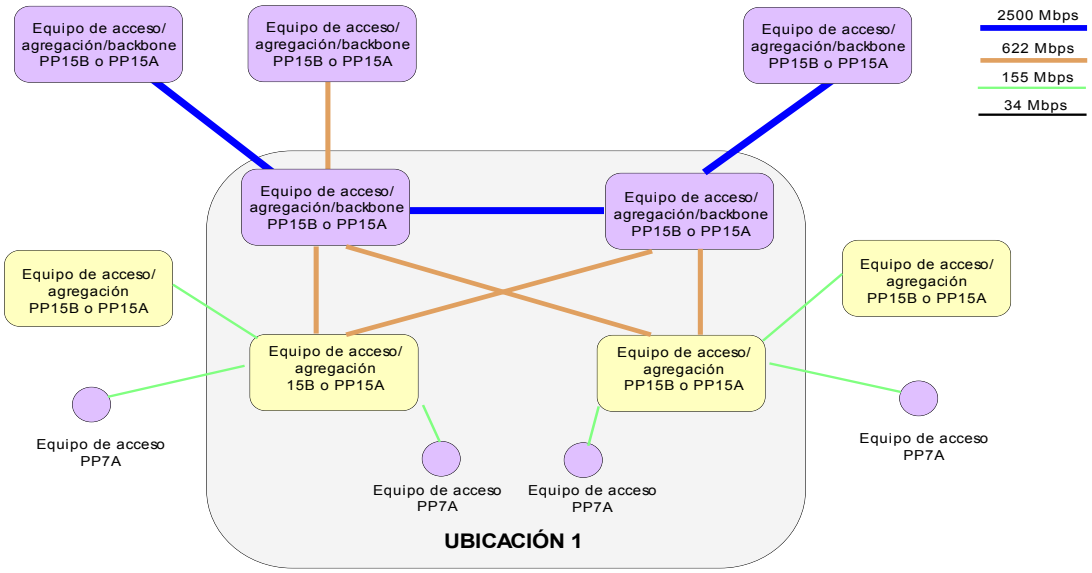


Figura 6.2.15 Niveles topológicos de la red ATM.Elaboración propia.

Actualmente en la red se encuentra desplegado el **PNNI jerárquico como protocolo de routing** del tráfico ATM, entre los equipos Ericsson. Las **conexiones de las estaciones base** con sus controladoras se realiza por medio de la **red de transporte SDH multiservicio de Telefónica**.

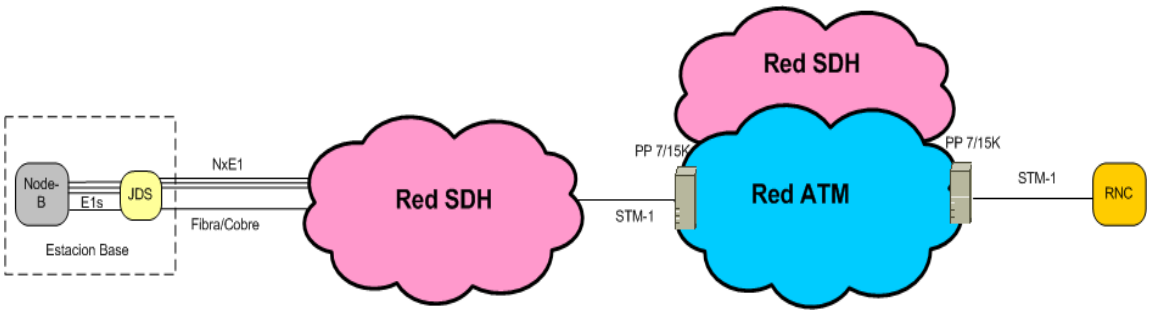


Figura 6.2.16 Esquema de conexión estación base con red ATM empleando la red transporte.Elaboración propia.

6.2.7.2 Transporte empleando las redes Ethernet MAN

Las redes Ethernet MAN se encargan de **trasportar los servicios móviles**, el **tráfico generado para UMTS** pero no de GSM como si hace la red ATM, y dará **conectividad con la red IP Única**. La conectividad de la estación base Nodo B con la controladora RNC utilizara la Red de Agregación Ethernet, donde los interfaces del Nodo B pueden ser de 10/100/Giga, siendo necesario en algunos casos ser necesario hacer uso de la Red de Transporte xWDM/SDH hasta llegar a un Nodo de la Red de Agregación Ethernet. La entrega del tráfico a las Controladoras Radio (RNC's) se realizara con interfaces 1/10 GbE de conexión con los nodos de la MAN. La estructura interna de la red MAN Ethernet ya está explicada en los apartados anteriores y se basa en tecnología de vlanes y VPLS.

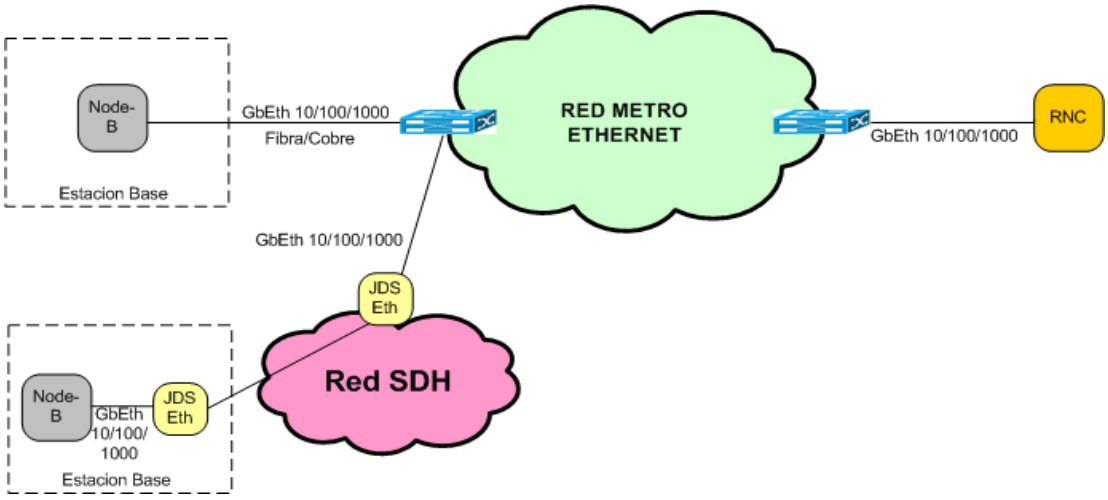


Figura 6.2.17 Esquema conexión estación base con red Ethernet usando la red transporte.Elaboración propia.

6.3 RED UNO/MULTISERVICIO

Tal y comente en la descripción general del punto 11.2.2 sobre la red UNO **es una red de nivel 2** con **tecnología ATM** que tuvo sus orígenes en la **red Iberpac de Telefónica** y que ofrece **servicios de redes privadas a clientes (RPV).** En esta ocasión pasare a analizar detalladamente su arquitectura, equipamiento y servicios que se ofrecen sobre dicha red.

6.3.1 Arquitectura de red

La Red Uno es una **red monovendor formada por equipos de Ericsson**. La red esta formada por **dos niveles**:

- **Acceso o agregación**: Está constituido por los Centros de Acceso y soporta los servicios y la conexión de los terminales de los clientes.
- **Backbone o malla central**: Es la parte troncal de la red, proporcionando capacidad de transporte e interconexión entre nodos.

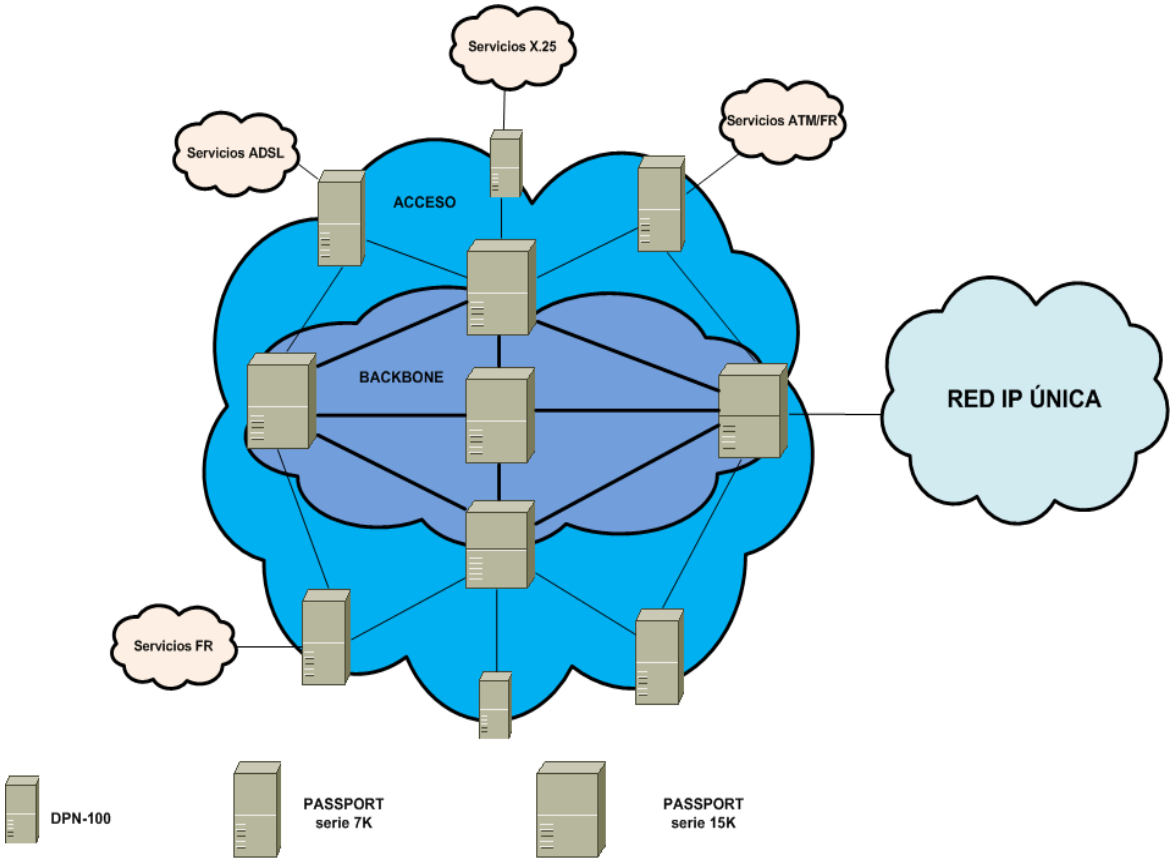


Figura 6.3.1 Arquitectura de red UNO en dos niveles. Elaboración propia.

El **backbone** está formado por **nodos Passport-15000** con capacidad de hasta 2,5 Gb, en el **acceso** se emplean **Passport de la serie 7000**, equipos **DPN para acceso y concentración de servicios X.*** y equipos **TEMIS como plataforma de respaldo FR**. Además los DPN's, se unen a la red UNO mediante enlaces de FR de 2Mb o UTP.

Los accesos tradicionales a la Red UNO desde las redes Ibermic, SDH y PDH, las velocidades oscilan entre los nx64 Kb a los 155 Mb. Se utilizan las **modalidades de acceso ADSL** para empresas **a través de GigaADSL**. Estos accesos se entregan mediante

PCC's en cada una de las localizaciones disponibles en la red GigADSL. Comentar que el acceso a través de la Red FR/ATM se realiza mediante líneas FR, ATM o líneas ADSL concentradas en los PCC's, distribuidos entre las demarcaciones GigADSL. **Los centros de acceso para Empresas de la red IP Única se conecta con la red UNO** en determinados centros para la entrega de clientes de servicios IP, en este caso la red UNO es la red de acceso/agregación para determinados servicios IP (VPN-IP).

La **red UNO tiene ámbito nacional** y presencia en **todas las provincias españolas**, y como ya he comentado, utiliza routing DPRS (para tráfico FR), PNNI jerárquico (para tráfico ATM) y PORS (para tráfico relacionado con aplicaciones en tiempo real). Cualquier caída de enlaces de red supone reenrutamiento dinámico de todas las conexiones. La red **está diseñada para que sea tolerante al fallo de cualquier nodo o enlace** ya que cada nodo de la Red se conecta como mínimo con otros dos.

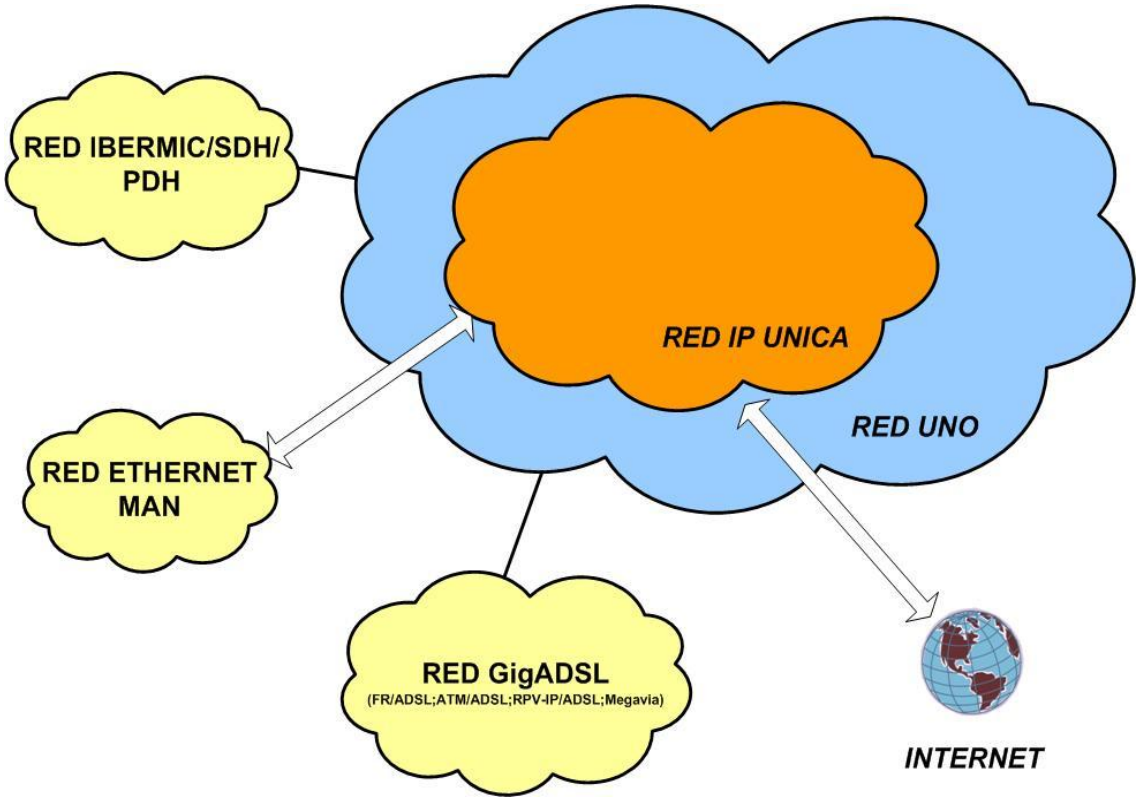


Figura 6.3.2 Esquema de interconexión de las diferentes redes con la red UNO. Elaboración propia.

6.3.2 Tipos de nodos de la red UNO

Conviene tener presente los siguientes términos cuando se hace referencia a la Red UNO:

- **Nodo**. Hace referencia a un equipo de alguna de las plataformas que componen la Red de Agregación ATM
- **Centro telemático**. Es un punto de la red en el que se realizan funciones de encaminamiento y consolidación del tráfico. Puede estar compuesto por uno (Ejemplo: Passport) o varios equipos o nodos (Ejemplo: DPN's y TEMIS).

Una vez realizada esta aclaración **los nodos que forman la red UNO** serian **DPN,PASSPORT,TEMIS**. Para conocer las caracterisiticas tecnicas y fisicas de estos equipos, **consultar el documento memoria_anex.pdf apartado ANEXO14.**

6.3.3 Tipos de accesos a la red UNO

Las conexiones a la red UNO se ofrecen basadas en diferentes protocolos y estándares tal y como muestra la figura.

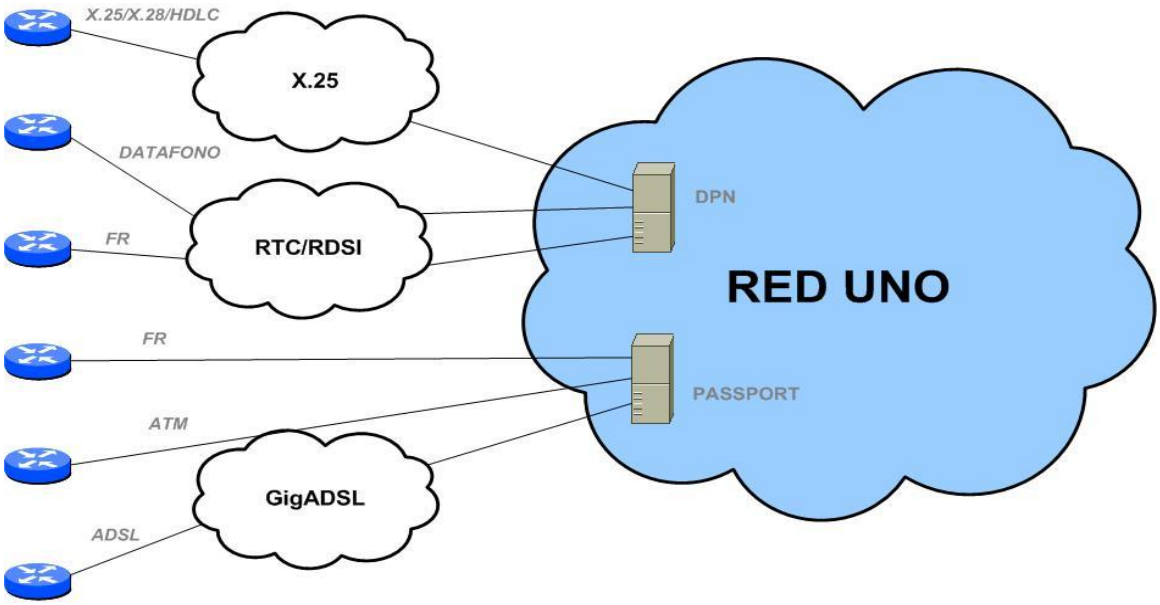


Figura 6.3.3 Tipos de accesos soportados sobre red UNO. Elaboración propia.

Para más información y arquitectura de los tipos de accesos a la red UNO consultar el documento memoria_anex.pdf apartado ANEXO15.

6.3.4 Servicios soportados sobre la red UNO

Los servicios soportados sobre la red UNO se pueden **clasificar en dos categorías** en función de si se ofrecen sobre el nodo de red DPN o Passport.

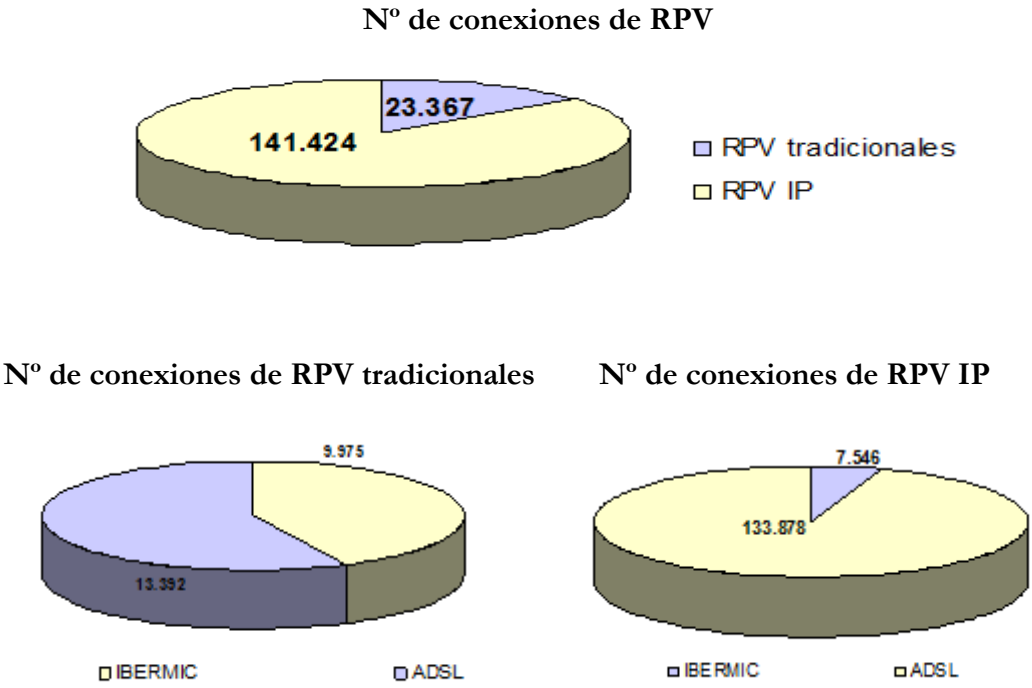
1) **Bajo el nodo de red DPN** se ofrecen los **servicios de red tradicionales de IBERPAC** que ya están prácticamente en desuso porque ya no se provisionan nuevos servicios bajo los DPN y los que existen se buscan emigrarlos a las nuevas arquitecturas de red bajo la Red IP Única.
    - Servicios X.25 (Iberpac, Iberpac plus)
    - Servicio Datafono
    - Servicio UNO
    - Servicio FR
2) **Bajo el nodo de red PASSPORT** se ofrecen **servicios de RPVs** basados en dos modalidades:

- **RPVs tradicionales**. Son servicios exclusivos de la red UNO basadas en tecnologías FR o ATM.
    - Servicio FR.
    - Servicio Interlan
    - Servicio Voz Interlan
    - Servicio ATM
    - Servicio CINCO
    - Servicio ViaSat
    - Servicio Nodo de Red

- **RPVs IP**: son servicios IP en el que la red UNO proporciona el acceso y transporte necesario para proporcionar el servicio final sobre los centros de acceso de la Red IP Única.
    - Servicio DataInternet
    - Servicio VPN-IP
    - Servicio Acceso a Intranet
    - Servicio Datafono ADSL

6.3.4.1 Demanda de los servicios

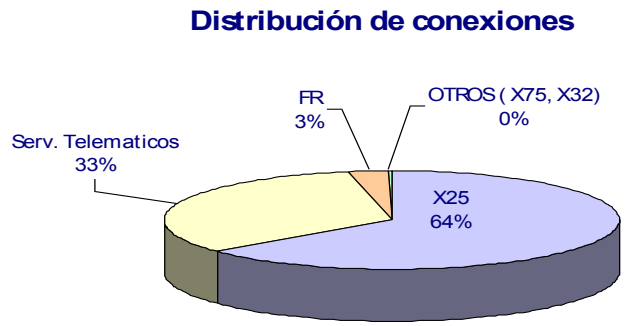
La evolución de la demanda de los servicios referentes a las RPVs en la actualidad se corresponde con el siguiente gráfico:



Gráfica 7.3.1 Número de conexiones actuales de RPVs. Elaboración propia.

Donde se observa que las **RPVs IP suponen el 86%** de las conexiones actuales frente **14% de las RPV tradicionales** y esto es así porque en la **actualidad no se provisionan nuevas RPVs tradicionales** y las que existen se están intentando migrar a infraestructuras de RPVs IP. También destaca que **la mayoría** de las **RPVs IP se provisionan sobre tecnología ADSL**.

Respecto a los **servicios tradicionales** que se proporcionan sobre los nodos DPNs, tal y como he comentado, tampoco **se provisionan nuevos servicios** y los que están, se intentan migrar a nuevas infraestructuras IP o ya ni se comercionalizan porque no existe solución alternativa. La distribución actual de los servicios tradicionales sobre las red UNO corresponde al siguiente gráfico.



Gráfica 7.3.2 Distribución actual de los servicios tradicionales sobre la red UNO. Elaboración propia.

6.3.4.2 Servicios tradicionales bajo nodo DPN

6.3.4.2.1 Servicios X.25

Son **servicios de transmisión de datos** basados en el **protocolo X.25** que utilizan los **nodos DPN** para conectarse a la red UNO para la **transportar los datos mediante CVP o CVC** con el extremo opuesto. Se ofrece en **dos modalidades denominadas Iberpac e Iberpac Plus**. Las características de ambos servicios son:

- **Velocidad** de acceso hasta **2 Mbits/s.**
- **Control sobre el uso de direcciones**: Grupo Cerrado de Usuarios, Grupos de captura, etc.
- **Capacidad de conexión** de todo tipo de equipos y plataformas que utilicen los protocolos X.25 y SDLC (SNA).

La diferencia de ambos servicios radica en que en **Iberpac se tarifica por uso y en Iberpac Plus es una tarifa plana** independiente del grado de utilización, que permite controlar el gasto en comunicaciones de las empresas.

Las aplicaciones que principalmente utilizan estos servicios son:

- Intercambio de tráfico transaccional
- Conexión de terminales a un ordenador central
- Correo electrónico

Las velocidades de acceso que ofrecen los servicios son:

- Dedicado X.25: 1.2, 2.4, 4.8, 11.6, 111.2, 64, 128, 256, 512, 1984 Kbit/s

- Dedicado HDLC-MNR: 1.2, 2.4, 4.8, 11.6, 111.2, 64, 128, 256 Kbit/s
- Dedicado DEP/PAD X.28: 1.2, 2.4, 4.8, 11.6, 111.2 Kbit/s (sólo Iberpac Básico)

Y las interfaces físicas que utilizan son las siguientes:

- Velocidades de 1.2 – 111.2 Kbit/s → V.24/V.28
- Velocidades de 64 – 512 Kbit/s → V.35
- Velocidad de 1984 Kbit/s → G.703/G.704

La estructura de red vendría representada en el esquema siguiente:

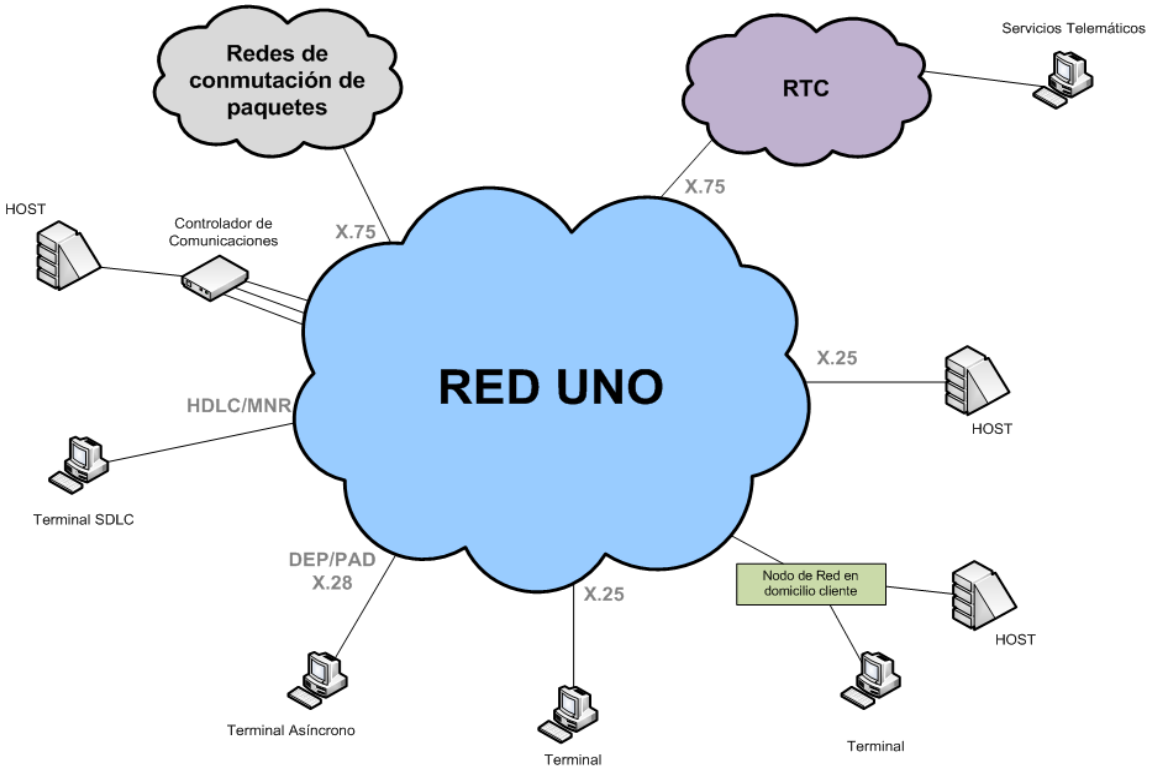


Figura 6.3.4 Esquema de los servicios X.* .Elaboración propia.

6.3.4.2.2 Servicio Datafono

El servicio Datafono es un **servicio telemático** que permite la conexión a la red UNO de **terminales tipo datafono conectados** a una RTB empleados para medios de pago efectuados con tarjetas de crédito o débito entre el TPV o Datafono y el ordenador central que gestiona este servicio. Los Datáfonos integrados en el servicio acceden a la Red UNO a través de la RTB mediante la **marcación previa del número 090** y se le tarifica como

una llamada metropolitana. Al destino (la central) se le factura el precio de uso de Iberpac, estando obligado por tanto a usar la modalidad de cobro revertido.

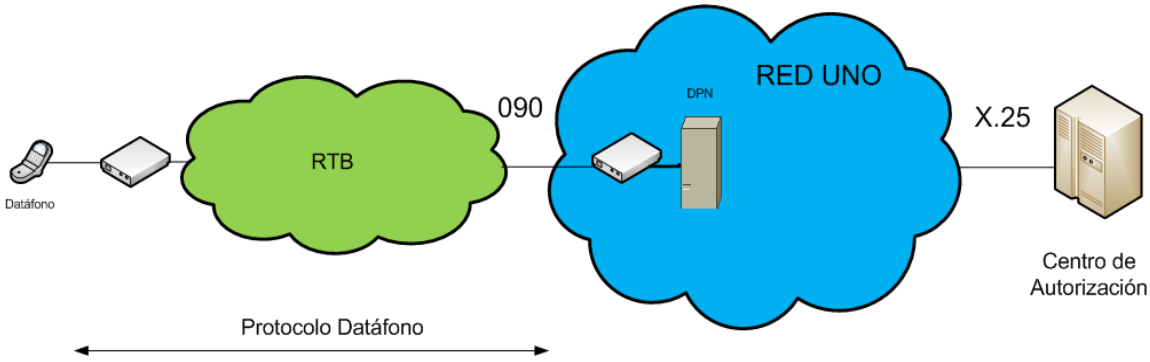


Figura 6.3.5 Esquema de conexión del servicio Datafono. Elaboración propia.

6.3.4.2.3 Servicio UNO

El servicio Uno, está basado en el **protocolo X.25** y en la filosofía de **Red Privada Virtual (RPV),** para ofrecer soluciones globales de transmisión de datos con cobertura nacional apoyándose en la red UNO. Gracias a este servicio, las grandes empresas pueden optar por diseños personalizados de red para comunicaciones de alta calidad. Este servicio ofrece las siguientes características:

- **Diseño personalizado** que hace posible dedicar los recursos de red con exclusividad.
- Se factura sobre una **tarifa plana** independientemente del tráfico cursado.
- Es posible introducir un **nodo de red gestionado** desde la propia empresa.

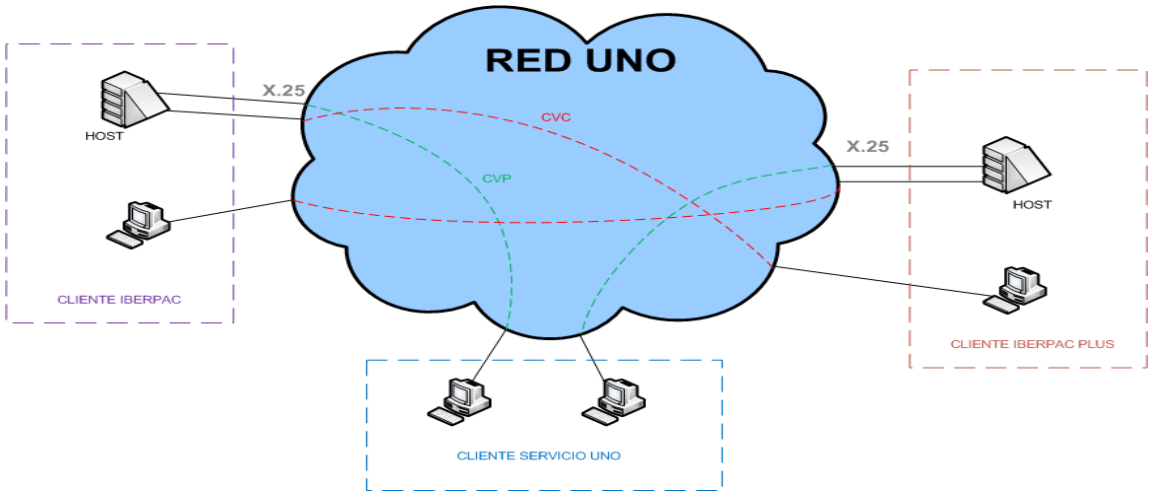


Figura 6.3.6 Esquema de conexión del servicio UNO. Elaboración propia.

6.3.4.2.4 Servicio FR

Es un servicio de **comunicaciones de datos a alta velocidad (de 64Kbps a 2Mbps)** bajo el protocolo **frame-relay** que permite la interconexión eficiente entre delegaciones de clientes repartidas geográficamente de diversos tipos, eliminando así las distancias entre oficinas y aumentando considerablemente el volumen de datos a transmitir.

El Servicio Frame-Relay se presta **en régimen de Red Privada Virtual**, mediante **Circuitos Virtuales** que pueden ser de dos tipos:

Permanentes: conexión permanentemente establecida entre sedes. El conjunto de CVP define la topología de la Red Privada Virtual. La incorporación de nuevas sedes o la interconexión de puntos no conectados se realizan fácilmente añadiendo nuevos CVP. Adicionalmente, existen los CVP Prioritario que consigue un retardo menor incluso en momentos de congestión mediante la asignación de una mayor prioridad de transporte en su recorrido por la red UNO.

Conmutados: conexión establecida y liberada previa señalización.

Frame-Relay permite la definición de conexiones lógicas de transporte ó DLCs con diferentes destinos, definidos para un mismo puerto de acceso. **Para identificar los distintos circuitos** dentro de una conexión física se utiliza el Identificador **DLCI (Data Link Connection Identifier).**

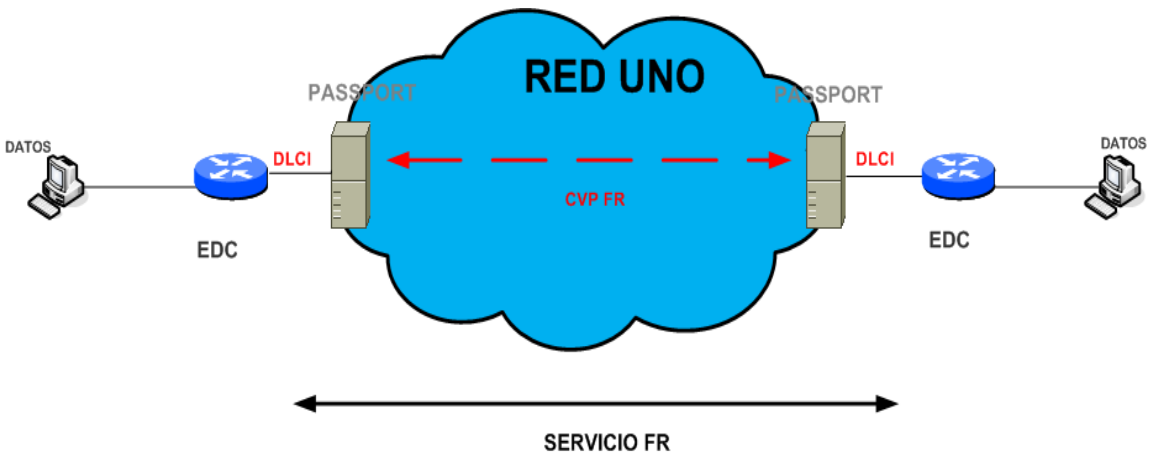


Figura 6.3.7 Esquema de conexión del servicio Frame-Relay. Elaboración propia.

Para poder satisfacer las necesidades de los diferentes clientes, el Servicio Frame-Relay ofrece **múltiples modalidades de acceso**:

- Circuitos digitales punto a punto.
- Canal B RDSI
- Respaldo de líneas de acceso por RTC y RDSI.

Como **complemento a la redundancia de caminos** y para evitar la incomunicación de la transmisión en caso de caída de los circuitos virtuales, el servicio Frame-Relay ofrece dos funcionalidades de red:

El CVP+: backup de un extremo del CVP.

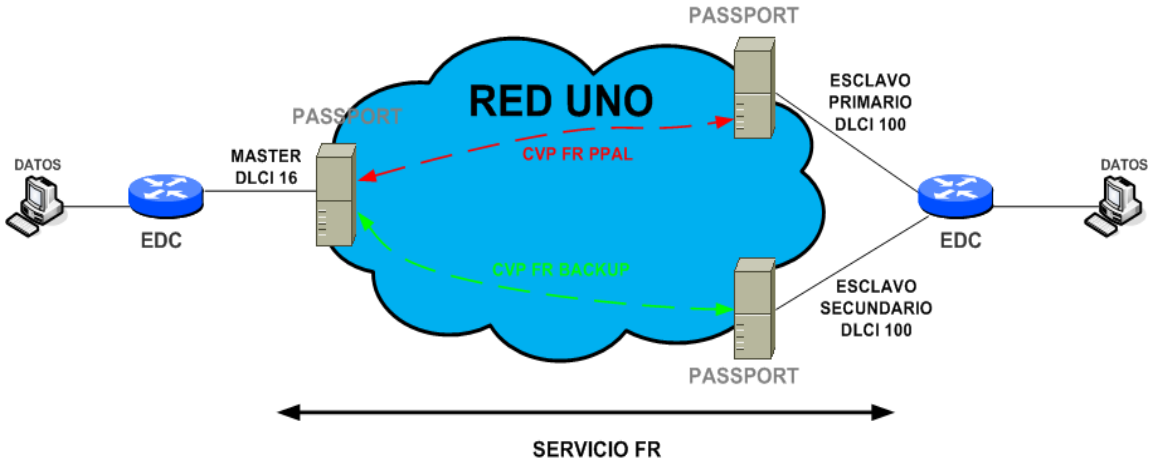


Figura 6.3.8 Esquema de la funcionalidad CVP+ del servicio FR. Elaboración propia.

Redirección+: proporciona un acceso alternativo de los puntos centrales de las RPVs.

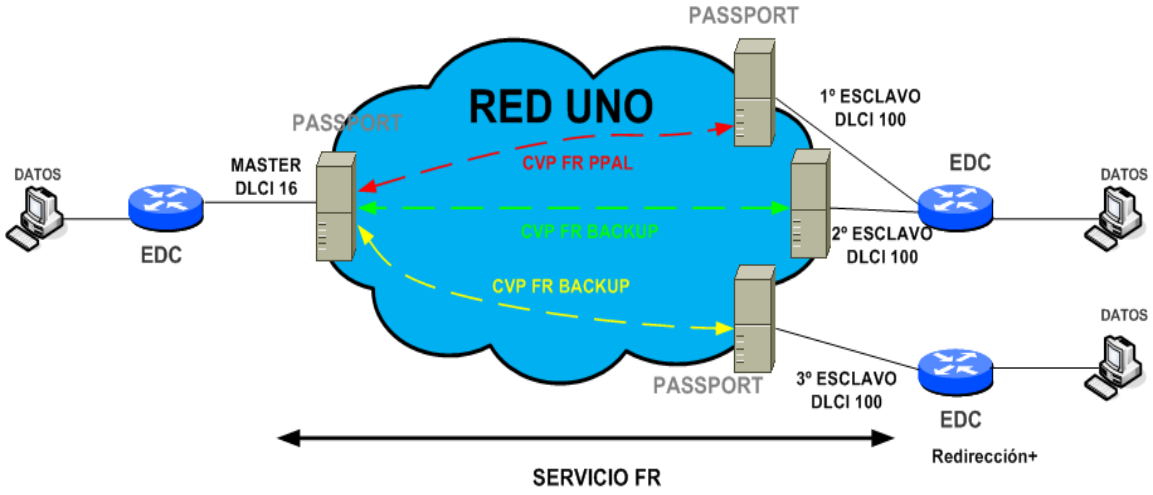


Figura 6.3.9 Esquema de la funcionalidad Redirección+ del servicio FR. Elaboración propia.

6.3.4.3 Servicios tradicionales bajo nodo PASSPORT

Como he comentado anteriormente, se ofrecen servicios bajos RPVs tradicionales y bajo RPVs IP. Los servicios sobre RPVs IP se explicaran más adelante cuando se trate la Red IP Única ya que estos servicios se apoyan en la red UNO para acceder a la Red IP Única, es decir, que la red UNO la utilizan de tránsito. Los servicios sobre **RPVs tradicionales** que todavía están en funcionamiento pero que **ya no se comercializan altas nuevas y se están migrando a IP** son lo que detallo a continuación.

6.3.4.3.1 Servicio FR

Es el mismo servicio **Frame-relay explicado en el punto anterior pero bajo los nodos de red Passport**. Esto implica que las tarjetas y velocidades que ofrecen los Passport son las siguientes. Para saber los tipos de interfaces y las velocidades de cada una de ellas **consultar el documento memoria_anex.pdf apartado ANEXO16.**

6.3.4.3.2 Servicio Interlan

El servicio Interlan es un **servicio de interconexión de redes locales** de una empresa sobre infraestructura compartida perteneciente a Telefónica que sería la red UNO y que ofrece la posibilidad de crear **una Red Privada Virtual** con las siguientes características:

- **Conexión permanente** y conmutada sin restricciones a la Red UNO.

- Permite la utilización de **direccionamiento IP público o privado**, o de protocolos distintos de IP.
- **Conectividad prefijada** entre oficinas corporativas seguras por medio de caminos virtuales permanentes (CVPs FR ó VCCs ATM).
- **Es un servicio gestionado**. Es decir, la gestión de los routers en las oficinas de cliente se realiza por parte de Telefonica y esta se realiza desde el centro de gestión, de forma remota.

Para crear estas RPV, se utilizan equipos routers en domicilio de cliente, que se conectarán a la red UNO mediante **accesos ADSL, ATM, FR y FR Canal B** explicados cada uno de ellos en el apartado 11.3.4 referente a los tipos de accesos sobre la red UNO. Posteriormente la conectividad entre estos circuitos se realizará con la utilización de caminos virtuales predefinidos. Lo que proporciona Interlan **es una RPV con topología en estrella** donde las oficinas remotas de una empresa se interconectan con la sede central donde se encuentran todos los servidores de comunicaciones. Todas las conexiones de bajo Interlan están siendo sustituidas por el servicio VPN-IP bajo la red IP Única.

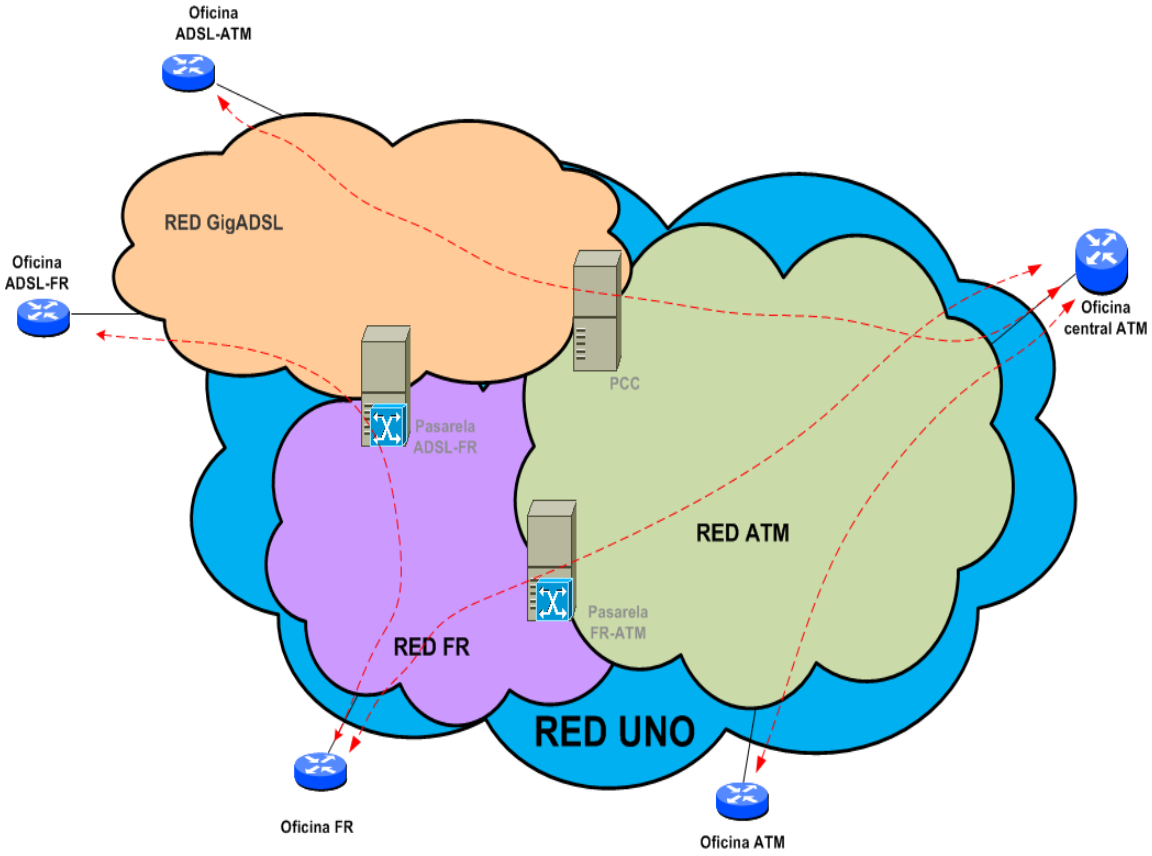


Figura 6.3.10 Esquema de red del servicio Interlan. Elaboración propia.

6.3.4.3.3 Servicio Voz Interlan

El servicio de Voz Interlan permite el **transporte de VoIP** definido sobre el la infraestructura del servicio InterLAN para integrar las comunicaciones corporativas de voz **suponiendo una reducción** de los **costes globales** de comunicaciones corporativas de voz y fax debido a la integración de las comunicaciones de voz sobre **infraestructura desplegada para las comunicaciones de datos**. Esto implica que contratar el servicio InterLAN Voz es indispensable haber contratado el servicio InterLAN. Aunque al igual que pasaba con Interlan ya no se permiten altas nuevas de estos servicios y los que existen se están migrando a VPN-IP.El servicio InterLAN Voz sólo contempla los elementos correspondientes al tráfico de voz. Las funcionalidades del servicio son las siguientes:

- **Comunicaciones de voz sobre IP** dentro del entorno corporativo, mediante CVP Prioritarios diferentes a los CVP para datos.
- **Comunicaciones de voz** con la RTB/RDSI

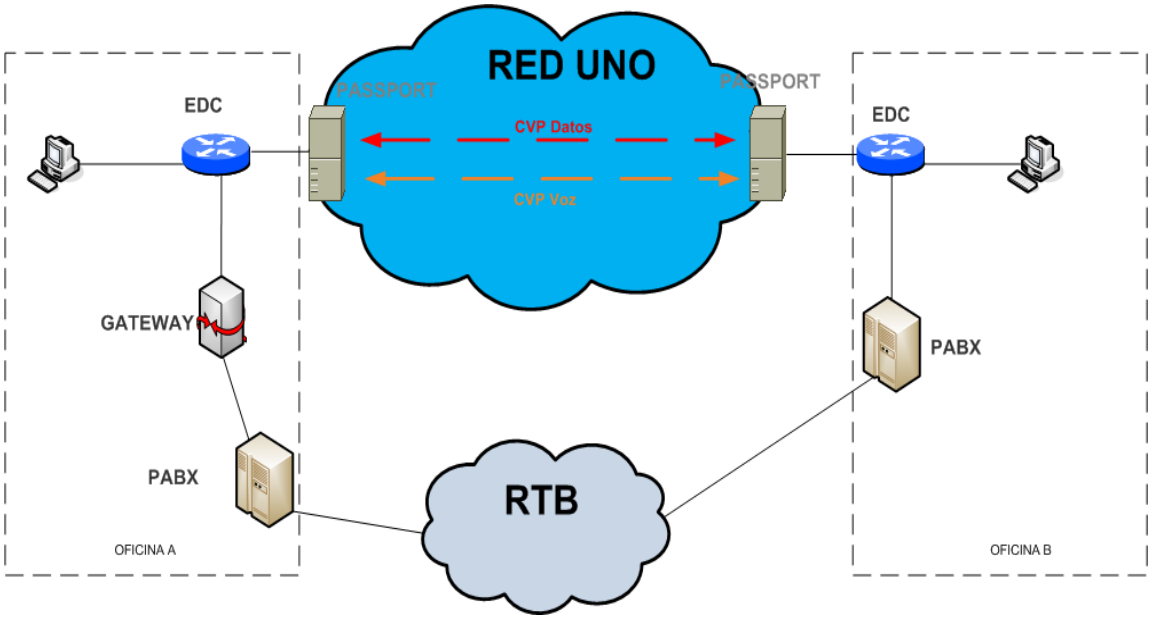


Figura 6.3.11 Esquema de red del servicio Interlan VOZ. Elaboración propia.

6.3.4.3.4 Servicio ATM

ATM es un servicio **de comunicaciones de datos a alta velocidad (hasta 155Mbps)** que permite la conexión eficiente, fiable y con mínimo retardo entre las diferentes instalaciones del cliente. Su capacidad multiservicio **permite el transporte de datos, voz e imágenes**, soportando cualquier tipo de aplicación multimedia. El Servicio ATM se presta en **régimen de Red Privada Virtual, mediante Circuitos Virtuales Permanentes**

(VCCs ATM) que permiten mantener múltiples comunicaciones con uno o varios destinos.

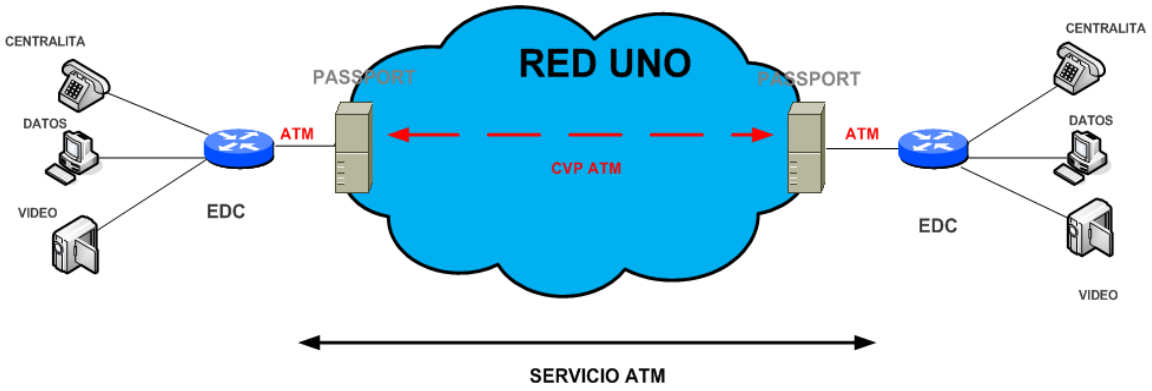


Figura 6.3.12 Esquema de red del servicio ATM.Elaboración propia.

Como características fundamentales del Servicio ATM destacan su alto rendimiento y elevada eficiencia, debido a:

- **Conmutación celdas ATM:** Las celdas son las unidades de transferencia de información y su longitud fija (53 octetos) permite que la conmutación se realice por hardware.
- **Única línea de transmisión:** La multiplexación estadística de las comunicaciones permite que en una misma conexión convivan diferentes canales.

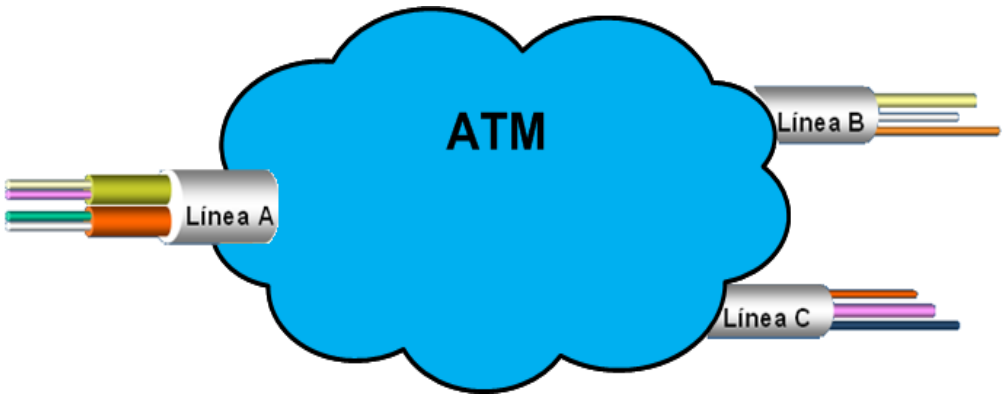


Figura 6.3.13 Multiplexación de canales sobre una misma conexión mediante VCC. Elaboración propia.

Para cumplir con los requisitos esperados de ancho de banda se emplean **dos tipos de calidades de servicio**: **VBR-rt y VBR-nrt. La explicación de cada una de ellas se puede consultar en el documento memoria_anex.pdf apartado ANEXO17.**

Entre las aplicaciones típicas para las que se puede utilizar el Servicio ATM se encuentran las siguientes:

- **Intercambio** de información en **tiempo real**, dentro del ámbito empresarial.
- Integración total de Redes de Área Local de la empresa que requieran gran ancho de banda.
- **Transmisión de voz** en entorno corporativo con compresión y supresión de silencios.
- **Acceso a Internet** a alta velocidad.
- Interconexión de centralitas.
- Transmisión de videoconferencia.
- Distribución en general de audio o vídeo.
- Transferencia de ficheros.
- Tráfico transaccional.

6.3.4.3.5 Servicio CINCO

El servicio CINCO (Comunicaciones Integrales Corporativas) es un **servicio multimedia** de transmisión de **voz, datos e imágenes sobre ATM** que pretende resolver de manera global las necesidades de comunicación del entorno corporativo. Se basa en el **concepto de Red Privada Virtual Multimedia** con recursos dedicados en exclusiva, **una infraestructura de red compartida** y un medio de acceso único a la red: servicios que hasta ahora se proporcionaban sobre redes distintas pueden ser consolidados en una única red, gracias al uso de un equipo integrador en domicilio del cliente. La diferencia con el servicio ATM radica en que la **gestión y mantenimiento del equipamiento** en el domicilio de cliente es realizada por **Telefonica** mientras que en ATM no.

6.3.4.3.6 Servicio ViaSAT

El servicio ViaSat es un **servicio de Red Privada Virtual** basado en la utilización de **tecnología satelital** ideal para aquellas empresas con dispersión geográfica nacional o internacional, que tienen necesidades de comunicación transaccional o difusiva. Se **apoya**

en satélites geoestacionarios para realizar la transmisión y recepción de la información sin limitaciones geográficas. Las antenas en tierra se comunican enviando la información en forma de energía electromagnética, que, al alcanzar al satélite, es devuelta nuevamente a tierra para los lugares de interés, sin que la existencia de montañas, edificios o ríos representen un obstáculo. Las antenas **en tierra tienen conectividad con la red UNO** y mediante CVPs se transportara el trafico hacia el resto de las sedes de la empresa. Sobre el servicio ViaSat se puede **transmitir simultáneamente voz y datos**. Los **protocolos de datos** para transmitir pueden ser **HDLC, X.25, IP**, etcétera, y se logra una muy alta eficiencia debido a la naturaleza estadística de la transmisión, que logra un perfecto equilibrio de economía en costos por transacción.

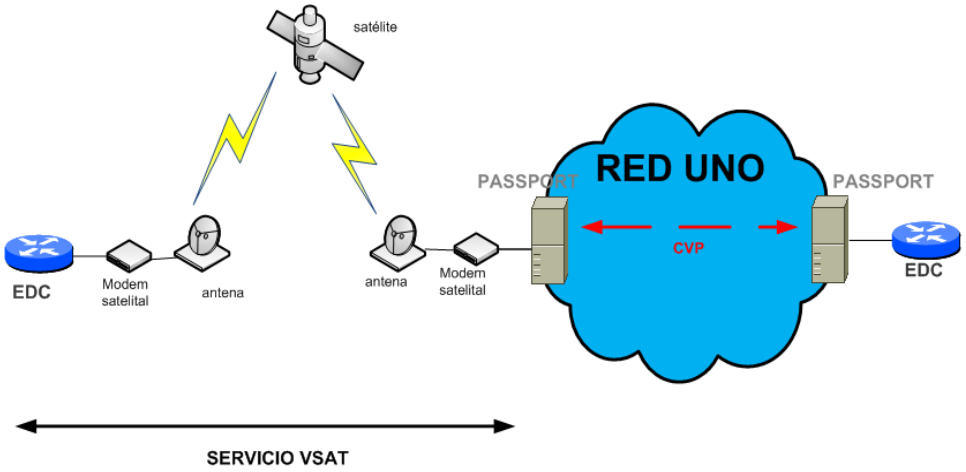


Figura 6.3.14 Esquema de red del servicio VSAT. Elaboración propia.

6.3.4.3.7 Nodo de Red

El servicio de Nodo de Red **es una plataforma física que se instalada en las dependencias del cliente** y **gestionada por Telefónica** que permite prestar diferentes servicios de transmisión de datos (**X.25, Frame-Relay o ATM**) sin que esto conlleve circuitos adicionales de acceso por cada servicio que se quiera contratar. Los tipos de enlaces que puede tener el nodo de red son:

- **Del Nodo de Red a la Red UNO**: los enlaces hacia la Red UNO tendrán titularidad de Telefónica y puede haber tantos enlaces como se desee por temas de redundancia o de reparto de carga, siendo dos el número mínimo recomendado.

- **De un Nodo de Red a otro Nodo de Red de su propiedad**: los enlaces entre Nodos de Red se asignarán a un determinado Nodo de Red. Enlaces entre un DPN y un Passport se asignarán al nodo de Red equipado con DPN. Estos enlaces pueden establecerse en Local (entre Nodos de Red ubicados en el mismo domicilio del cliente) o bien mediante líneas punto a punto. Dichas líneas serán titularidad de Telefónica.

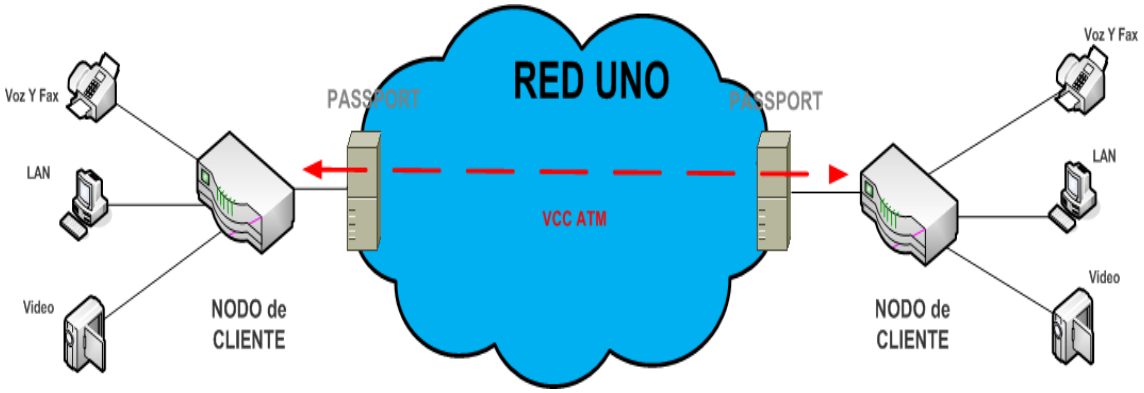


Figura 6.3.15 Esquema de red del servicio Nodo de Red. Elaboración propia.

6.4 RED IP UNICA

La Red IP Única es un proyecto que ha venido desarrollándose en los últimos años en base **a las tres redes IP de Telefónica** con son:

- **RUMBA**: es la red IP para grandes clientes de Telefónica que proporciona servicios de acceso a Internet y de RPVs.
- **RIMA**: es la red IP para el transporte IP/MPLS del mercado de residencial y PYMES.
- **RUD**: es la red IP de móviles para el transporte de tráfico de datos 2/3G.

Con el objetivo de **unificar en una solo infraestructura** de red para el soporte de los servicios multimedia convergentes fijo-móvil ya que estas redes van evolucionando progresivamente a arquitecturas NGN con transporte de flujos de voz y señalización sobre IP. Los puntos claves para desarrollar la red IP Única son:

- **El soporte de todo tipo de servicios multimedia** vía servidores de aplicación.
- El **control de los terminales y sus sesiones** vía una capa de control común (IMS-Softswitch) y una base de clientes unificados.

- El transporte vía una red **"todo IP"** común.
- El acceso **banda ancha, sobre cobre, fibra o radio**.
- Soporte a los **terminales multimedia**.

Adicionalmente a la unificación de las tres redes IP anteriormente comentadas se ha implantado un **Anillo Critico IP** que es una infraestructura IP adicional que, como parte integrante de la red única, se especializa en atender **los tráficos más críticos** como son:

- **Señalización**
- **Voz Fija y Móvil**
- **Conectividad Sistemas de Explotación** de las Redes
- Conectividad de ciertas Plataformas SVA Fija y Móvil

La infraestructura Anillo Critico IP se diseñó con los más altos parámetros de eficiencia y seguridad, basando su estabilidad tanto en equipamiento y funcionalidades tecnológicas plenamente probadas, como en la separación clara entre el anillo y el ámbito de Internet y la baja operatividad sobre ella, ya que no se permite la provisión de clientes. Por tanto, el modelo actual de la red IP Única, tal y como se comentó anteriormente está compuesto por:

1. **La unificación de tres redes IP (RIMA,RUMBA,RUD)** de altísima capacidad, disponibilidad, con tratamiento específico y diferenciado de los tráficos en función de su criticidad y abierto a Internet.

2. **Un anillo critico IP** de alta capacidad y con alta seguridad estructural, aislado del mundo Internet y dedicado a soportar el tráfico sensible (con requisitos de gran disponibilidad) y altamente crítico para el negocio.

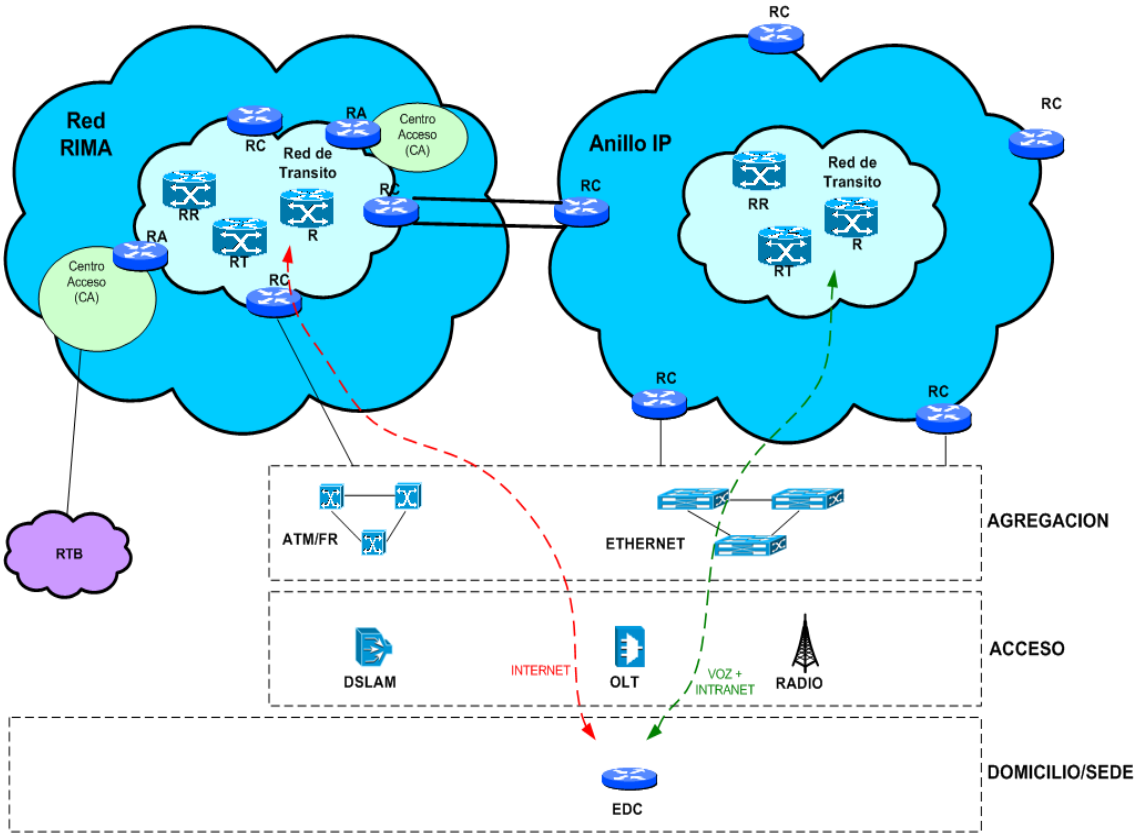


Figura 6.4.1 Esquema de red de integración del Anillo IP en red IP Única. Elaboración propia.

6.4.1 Criterios de diseño aplicados para el desarrollo de la red IP Única

Los criterios de diseño que se tuvieron en cuenta a la hora de desarrollar la Red IP Única se centraron en los siguientes aspectos:

1) ESCALABILIDAD

- Dimensionado de red para caudales medios muy superiores a los utilizados hasta ahora en las redes de Telefónica y en las terminaciones nacionales e internacionales de Internet.
- Capilaridad de la red elevada para atención rápida de crecimiento de la demanda en zonas con poca penetración de Internet.

2) CALIDAD

- Transporte de alta capacidad dedicado entre nodos (JDS, WDM).
- Alta capacidad y alta disponibilidad de transporte, conmutación IP (GigaRouters en Núcleo): IP directamente sobre SDH y en algunos casos sobre GigabitEthernet.
- Caching en Centros de Acceso.

- Navegación sin entunelado.
- Soporte de esquemas de clases de servicios en Routers y servidores de Acceso (RAS-RTB y BRAS) y, sobre todo, en routers de conexión a terminaciones nacionales e internacionales de Internet.
- Soporte de la clase de servicio específica para tiempo real.
- Utilización de Accesos Primarios para conexión con RAS.

3) FIABILIDAD

- Redundancia de equipos e interfaces.
- Balanceo de carga y mecanismos de reencaminamiento.
- Esquemas de protección MPLS.

4) FLEXIBILIDAD

- Red Abierta, con alta capacidad de crecimiento y de introducir nuevos servicios en base a la utilización de interfaces estándar reales o de facto.
- Arquitectura basada en productos comerciales, preferentemente "Plug-in".
- Capacidad por soporte de RPVs IP y teletrabajo.
- Soporte de multicast en red y en routers de conexión para conexión a redes externas.

Y para incluir un **Anillo IP Critico** que forme parte de la red IP Única para el transporte de tráfico crítico se desarrollo con el objetivo de **garantizar la continuidad del servicio incluso ante situaciones de fallo doble** en la red de transporte y con las siguientes premisas:

- **Seguridad lógica**: Es una red sin servicio ni interconexiones con Internet, por tanto es una red blindada por diseño ya que tiene un Sistema Autónomo Privado con direccionamiento IP no alcanzable desde el exterior.
- **Arquitectura homogénea y muy estable**: los equipos que se instalan en cada nivel de la red son del mismo modelo, con un HW y SW probados previamente.
- **Alta Conectividad**: es una estructura muy mallada en el nivel de Tránsito MPLS y en acceso (Malla de nodos de Acceso), de este modo siempre hay caminos IP alternativos ante cortes múltiples en la red de transporte.
- **Calidad**: Bajos niveles de retardo y jitter.
- **Ocupación máxima de enlaces del 35%,** de modo que exista vacancia suficiente en los enlaces para poder asumir el tráfico desbordado cuando se producen cortes múltiples en la red de transporte que afectan a varios enlaces de red.

- **Malla de acceso:** establecimiento de enlaces directos entre de centros de acceso que intercambian mucho tráfico para disminuir los retardos, además de proporcionar una seguridad adicional al establecerse estos enlaces IP por la tercera ruta de transporte.
- **Bajo nivel de intervención** en red para tratar de evitar los errores humanos:
- Provisión de servicio limitada a equipos de otras redes a los que se proporciona transporte IP, esto implica una baja intervención sobre los equipos al no tener que provisionar usuarios finales.
- **Máxima eficiencia:** Red de transporte dedicada tanto para servicios de Móviles como de Fijo.
- La **topología de la red** está ajustada a la naturaleza del tráfico que se transporta, que es tráfico de voz que se resuelve en un alto porcentaje (70%) a nivel provincial.
- **Redundancia y Seguridad**: Elementos IP redundados y mecanismos de convergencia rápida (IP Fast Reroute).
- **Routers reflectores** en todas las áreas de tránsito.
- Uso de la 3ª ruta de la RTLD para proporcionar supervivencia 100% del tráfico ante cortes dobles en transmisión.

6.4.2 Arquitectura de red de alto nivel

La arquitectura de la **red IP Única** se basa en un modelo de **dos capas: la capa exterior, o de acceso e interconexión, y la capa interior (o nivel troncal)**. Estas dos capas, junto con la red de gestión, constituyen los elementos principales de la red. Como he indicado anteriormente, la red IP Única está formada por la suma de las tres redes IP (RIMA, RUMBA, RUD) de Telefónica cuyo nombre del conjunto de las redes es **RIMA y el Anillo Critico IP** por lo que voy a **analizar estas dos arquitecturas por separado**.

6.4.2.1 Arquitectura de red RIMA

6.4.2.1.1 Nivel de Acceso

El nivel de **acceso** está **estructurado en demarcaciones.** Cada **demarcación tiene un Centro de Acceso (CA)**. Los usuarios pueden acceder a la red a través de la red conmutada (RTB o RDSI) o a través de accesos dedicados ADSL. Los CAs realizan la función de **concentración de los usuarios**, tanto conmutados como permanentes. Los

CAs se unen a la red troncal mediante un enlace doble: cada uno de los dos routers de acceso (RAs) que existen en los centros de acceso se conecta a dos routers de tránsito (RTs) diferentes.

Los **equipos de acceso** realizan las funciones de **agregación**, como terminación de **conexiones PPP**, agregación de líneas alquiladas, terminación **de conexiones ADSL y acceso a las redes privadas virtuales**. Además, en **ellos reside toda la complejidad** que conlleva el desarrollo de los requisitos de **calidad de servicio** que se vayan a implementar en la red, la definición de los usuarios que constituyen cada una de las redes privadas virtuales y las funciones de seguridad inherentes a ellas. Están constituidos por:

- Uno o varios equipos **RAS** para la interconexión con la red conmutada.
- Uno o varios equipos **B-RAS** para la interconexión con los PCCs ADSL.
- **Switch de nivel 2** (redundante) para la comunicación entre los diferentes elementos del CA. También realiza la función de interceptor para el caching.
- **Conmutador de nivel 2** para la red de gestión.
- **Router de Acceso (RA)** (redundante).
- **Servidores (Caching, DNS, LDAP,…).** Los CAs proporcionan la infraestructura necesaria para ofrecer los servicios que se prestan de manera distribuida. Todos los CAs incorporan caché de contenidos (para mejora de respuesta en acceso a Internet), pero sólo algunos de ellos (por pares) tienen servidores DNS, RADIUS y LDAP de ámbito nacional.
- **Router de consolas** para gestionar cualquier equipo del CA.

Para una información mas detallada de las arquitecturas y equipamientos empleados en los Centros de Acceso, consultar en el documento memoria_anex.pdf apartado ANEXO18.

6.4.2.1.2 Nivel de Tránsito

La red troncal o de tránsito de la red RIMA está **constituida por routers de tránsito (RT) de alta capacidad de conmutación: los Giga Switch Routers (GSRs)**. Los RTs se conectan entre sí en función de la demanda de tráfico entre nodos, formando una **red parcialmente mallada**.

Para reducir la carga de encaminamiento, se utilizada **MPLS como tecnología de conmutación** en la red de tránsito. En ella, el encaminamiento de los paquetes se basa en la **conmutación de etiquetas** de longitud fija asignadas a cada uno de ellos. Los **RA** son los encargados del **cálculo de las etiquetas** y del proceso de traslación entre paquetes IP y tramas MPLS. Los **RT se comportan como conmutadores de etiquetas (LSR)**. De esta forma el backbone central se estructura como una nube de tránsito MPLS, lo que permite una capacidad de enrutamiento mucho mayor que los sistemas tradicionales.

6.4.2.1.3 Nivel de interconexión

La conexión de la Red RIMA a otras **redes de otros operadores nacionales y con la red Internacional** se realizará a través de un **Router de Conexión (RC)** o, eventualmente, a través de un **Router de Acceso (RA)**, dependiendo del volumen de tráfico. En todos los casos, se utilizará el **protocolo BGP-4** para transferir la información de routing con técnicas de marcado y filtrado de direcciones

6.4.2.1.4 Red de Gestión

El **tráfico de gestión de la red se confina en una red privada virtual** específica para las máquinas de gestión que se extiende a todos centros de gestión. En ella se incluyen las redes de gestión de todos los centros de acceso y la red del centro de gestión. El tráfico de gestión proveniente de routers de acceso, RAS, BRAS y máquinas con servidores se recogerá sobre un conmutador Ethernet, que implementará una subred de gestión.

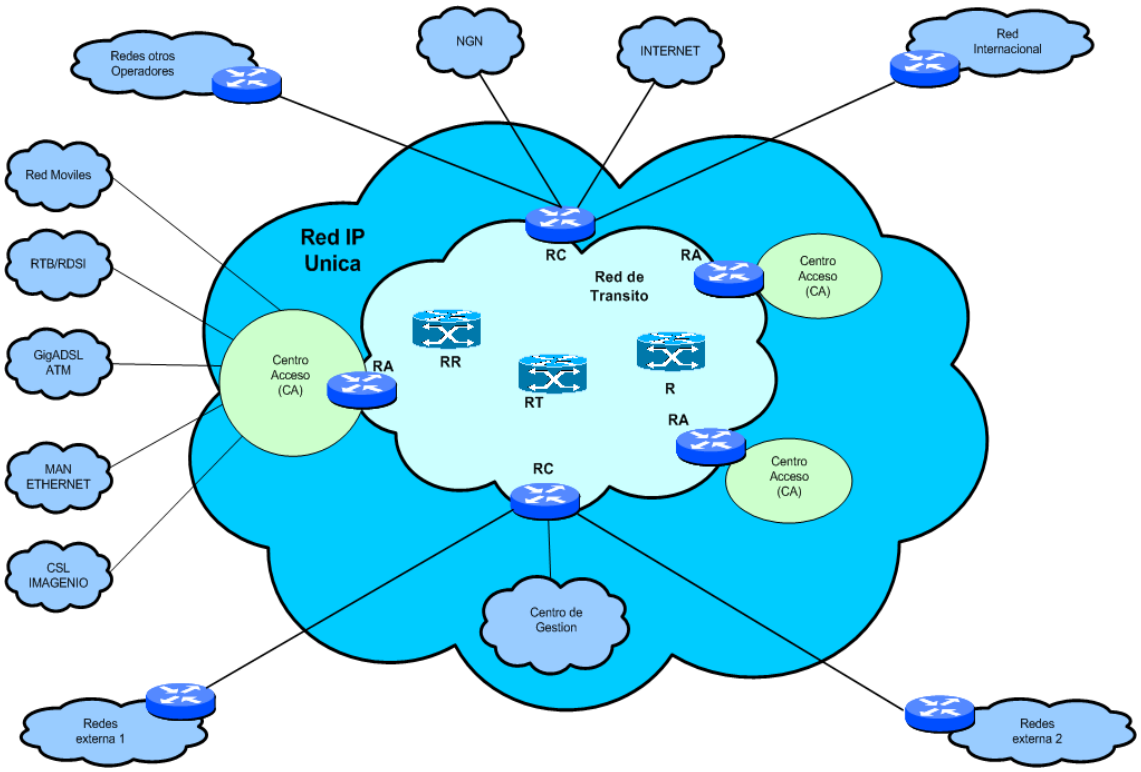


Figura 6.4.2 Arquitectura de la red RIMA. Elaboración propia.

6.4.2.2 Arquitectura de red Anillo Crítico IP

La **arquitectura** de red del Anillo está **condicionada** por las necesidades de **capilaridad, capacidad y seguridad del tráfico** que generen los diferentes servicios que van a hacer uso de él. Tendrá **cuatro niveles de red** diferenciados funcionalmente, **acceso, tránsito, interconexión y gestión** al igual que la red RIMA. Los niveles de acceso e interconexión compartirán infraestructura física.

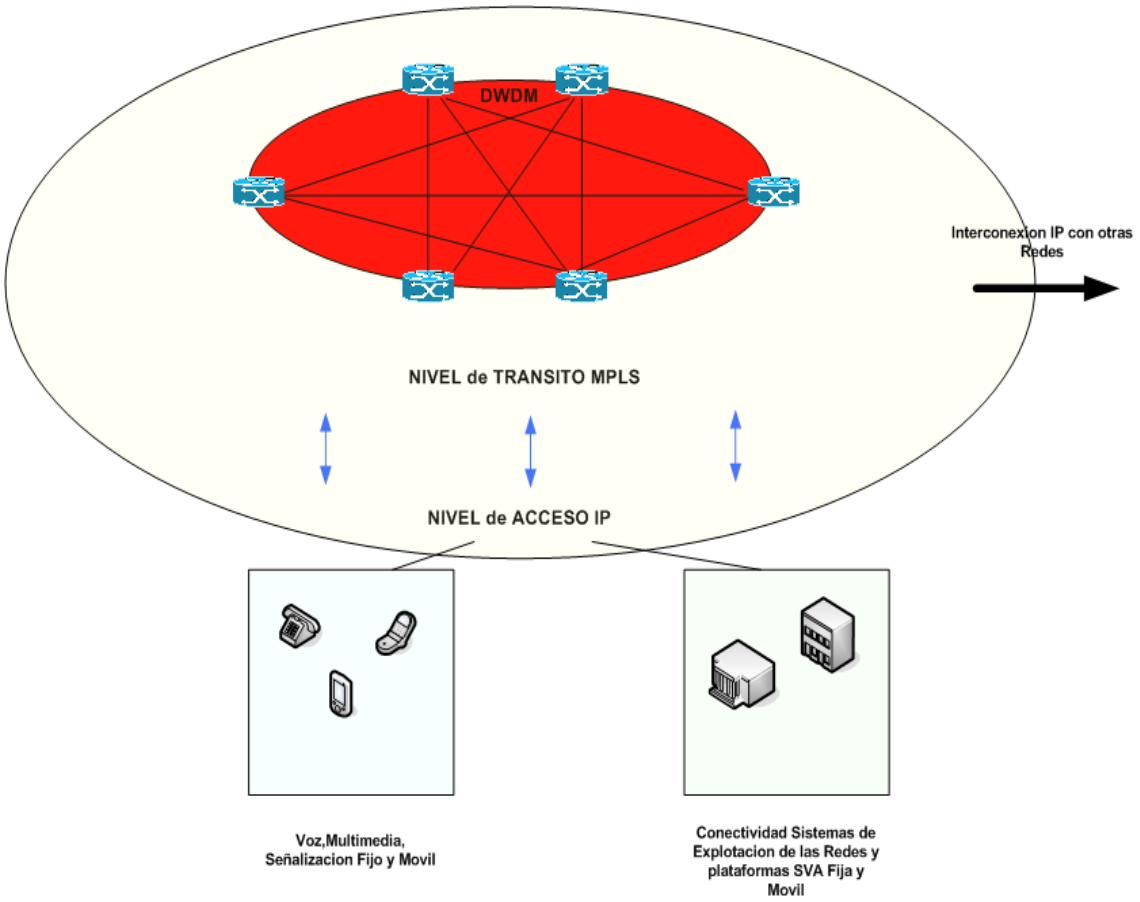


Figura 6.4.3 Arquitectura del anillo critico IP. Elaboración propia.

6.4.2.2.1 Nivel de Acceso

El nivel de **acceso** también está **formado por los Cas**. De forma general, los Cas Anillo IP estarán formados por una **pareja de routers** con un único nivel de conmutación que agregará las funciones de routing IP y conmutación/concentración Ethernet. Se caracterizarán por tener la siguiente conectividad:

- **Externa**. Por necesidades de capacidad, la conectividad a nivel 3 con el nivel de tránsito, entre routers de acceso del mismo CA y entre routers de acceso de diferentes Cas se implementará con interfaces de tipo POS STM-1, STM-4 y STM-16.
- **Interna**. Al unificar en un solo equipo las funcionalidades de nivel 2 y 3, la única conectividad interna necesaria se resume en cuatro conexiones GE, dos para facilitar la comunicación entre routers de acceso a nivel de switching y dos para tráfico de usuario.

- **Equipos de cliente**. Conectividad de tipo Ethernet (fibra y cobre)
  - Cliente ToIP FTTH (Voz sobre fibra 1ª línea).
  - Cliente RTB ó PSTN evolucionada hacia arquitectura basada en Softswitch.
  - Cliente Señalización Móvil (SIGTRAN).
  - Cliente Transporte de VoIP Móvil (Circuitos).

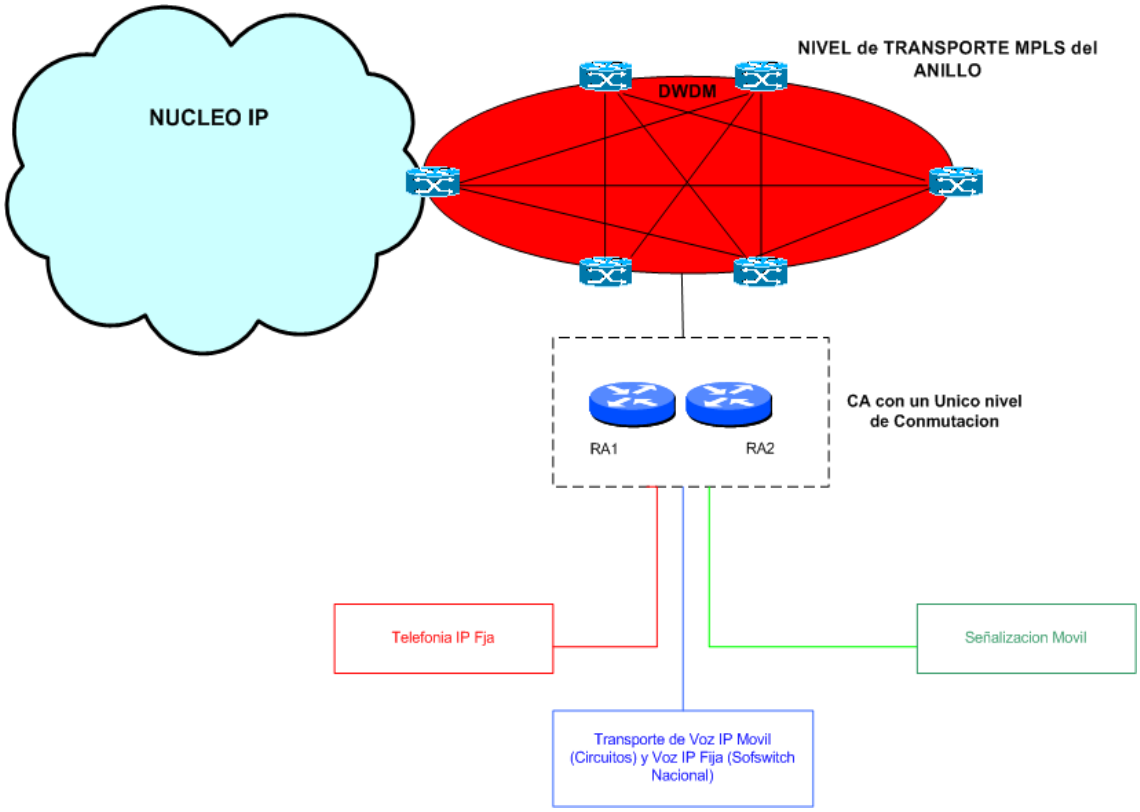


Figura 6.4.4 Arquitectura del CA del anillo IP crítico. Elaboración propia.

Los CAs están clasificados según los servicios que soporten, así un CA del Anillo puede ser: Centro de Gestión del Anillo, Centro de Gestión de NGN, Centro de Acceso de NGN principal o redundante, Punto de Presencia de NGN, Centro de Red de NGN, Centro de Acceso de Señalización Móvil, Centro de Acceso para Transporte de VoIP Fija y Móvil (Circuitos) o cualquier combinación entre ellos.

6.4.2.2.2 Nivel de Tránsito

El nivel de tránsito es el encargado de **conmutar a nivel MPLS los flujos de tráfico** sobre **una estructura en malla en la capa IP**, adaptada en su totalidad a la capa de transmisión.Cada centro está formado por una pareja de equipos conectados entre sí, cuya función será agregar y distribuir el tráfico interprovincial proveniente de su área de accesos

asociada a través de la malla MPLS hacia el resto de áreas. La arquitectura del tránsito se identificará por tener **dos estructuras malladas superpuestas formadas por enlaces STM-16 ó STM-64**. Como resultado se tiene una **arquitectura redundante, de gran robustez y seguridad**.

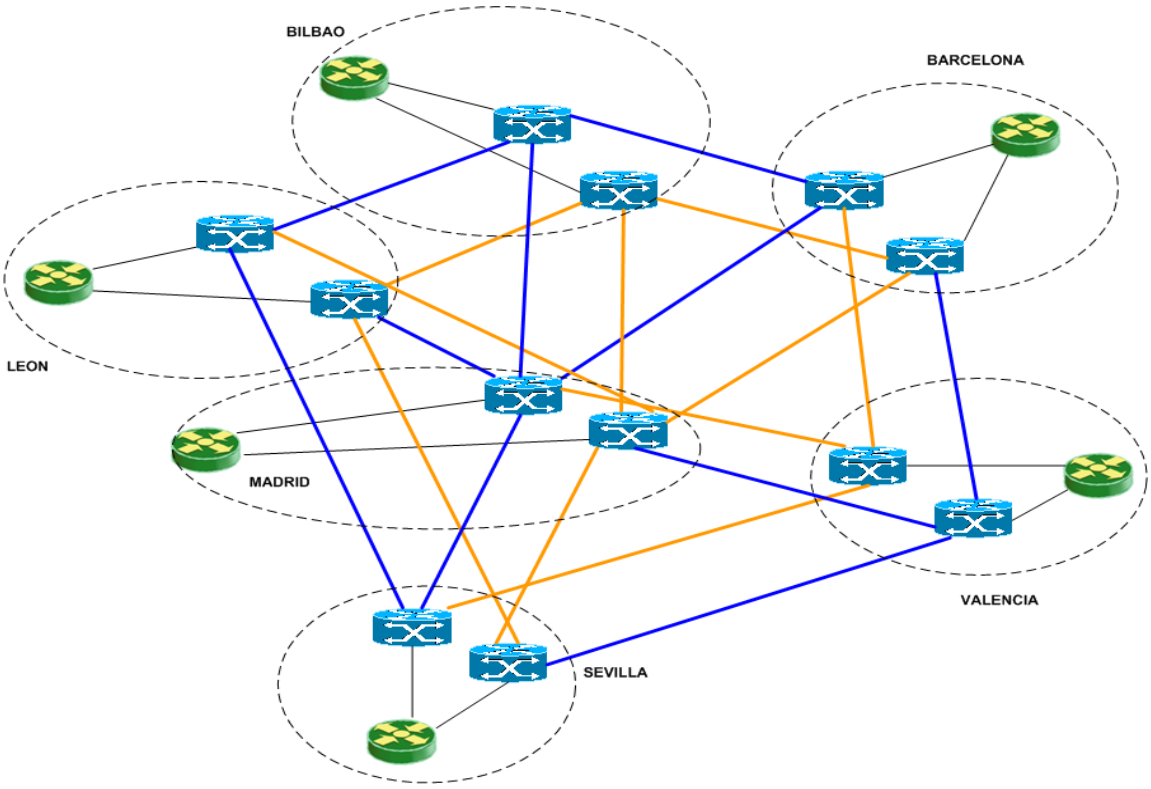


Figura 6.4.5 Arquitectura del nivel de tránsito del anillo IP. Elaboración propia.

6.4.2.2.3 Nivel de Interconexión

Es necesario tener interconexiones entre el Anillo IP y las diferentes redes IP (RIMA,RUMBA,RUD) que actualmente soportan los servicios involucrados en el proyecto, NGN FTTH y Sofswitch nacional e internacional, NGN Móvil, Señalización y Circuitos. Se **usarán gigas de unión en las interconexiones**, se usará el método de Inter-AS opción A. **Existirán tantas vlan como vrfs (Virtual Routing Fordwarding) se quieran anunciar entre las redes, y una sesión BGP por cada vlan.**

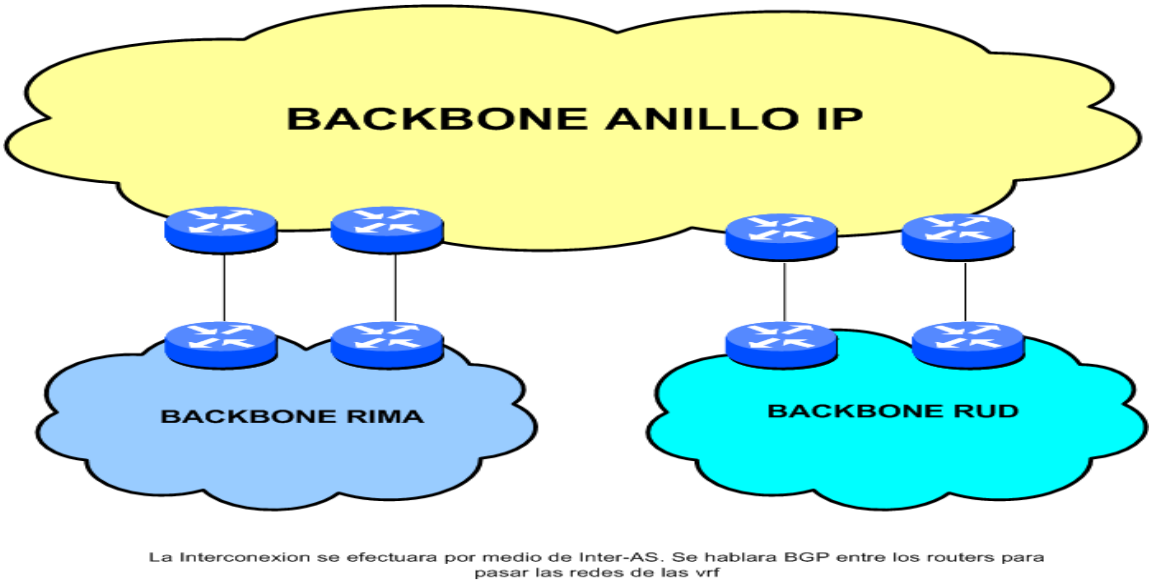


Figura 6.4.6 Esquema de interconexión del anillo con las redes IP. Elaboración propia.

6.4.2.2.4 Red de Gestión

Se emplea la misma red de gestión que se utiliza para gestionar los elementos de la red RIMA.

6.4.3 Arquitectura detalla de la red del nivel de tránsito

La arquitectura de **tránsito se basa en un modelo de dos capas**. La capa **interior o backbone** que se implementa con routers de nueva generación capaces de conmutar paquetes a altas velocidades, siguiendo los principios que impone la **tecnología MPLS (Multiprotocol Label Switching)** y la capa **exterior o de acceso** que se implementa con routers específicos de borde que adaptan el tráfico IP a tráfico capaz de ser conmutado en el interior de la red MPLS.

Los routers de borde soportan los protocolos definidos en el estándar MPLS, de modo que la red se implemente como una red IP/MPLS a fin de poder ofrecer un transporte del tráfico IP basado en **conmutación de etiquetas y los servicios de valor añadido, como ingeniería de tráfico**, propios de esta tecnología. Al tratarse de una arquitectura basada en MPLS sigue las recomendaciones que se implementan en la RFC 3031 aprobada por el

IETF. En la figura se aprecia el modelo de red IP/MPLS tal como se ha definido anteriormente.

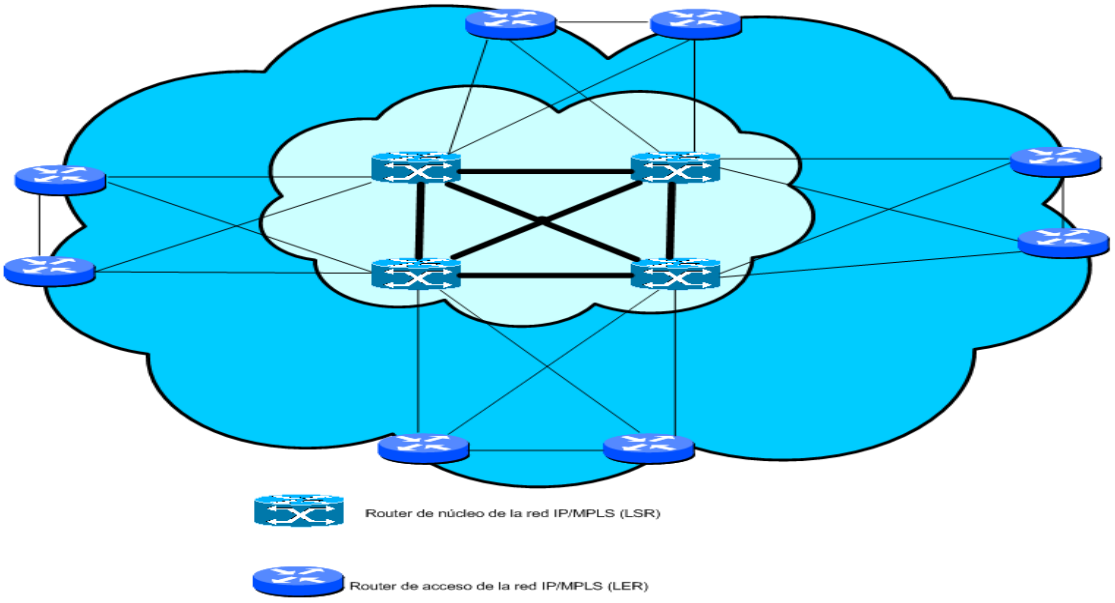


Figura 6.4.7 Modelo de red IP/MPLS. Elaboración propia.

Los centros de acceso realizan las funciones de agregación, como terminación de conexiones PPP, agregación de líneas alquiladas, terminación de conexiones ADSL y acceso a las redes privadas virtuales. Además, en ellos reside toda la complejidad que conlleva el desarrollo de los requisitos de calidad de servicio que se vayan a implementar en la red, la definición de los usuarios que constituyen cada una de las redes privadas virtuales y las funciones de seguridad inherentes a ellas. **Los routers de conexión proporcionan la interconexión con otras redes**: salida internacional, salida nacional a otros operadores, salida a Internet. Los equipos que componen el núcleo de la red (routers de tránsito) están dedicados al encaminamiento de paquetes I. De esta manera, **el núcleo está optimizado y dedicado a la transmisión de alta velocidad**.

El backbone de la red RIMA está constituido por **centros de tránsito** de altas prestaciones, **centros de acceso** que trabajan en condiciones de reparto de carga, **routers de conexión** que proporcionan la conexión con servidores ajenos a la arquitectura de la red RIMA y **reflectores de ruta** también trabajando en condiciones de reparto de carga que se encargan, exclusivamente, de distribuir la información de routing al resto de routers que componen la red. Los reflectores de rutas no conmutan tráfico y sólo se encargan de recibir y anunciar rutas BGP. El esquema detallado se muestra en la siguiente figura.

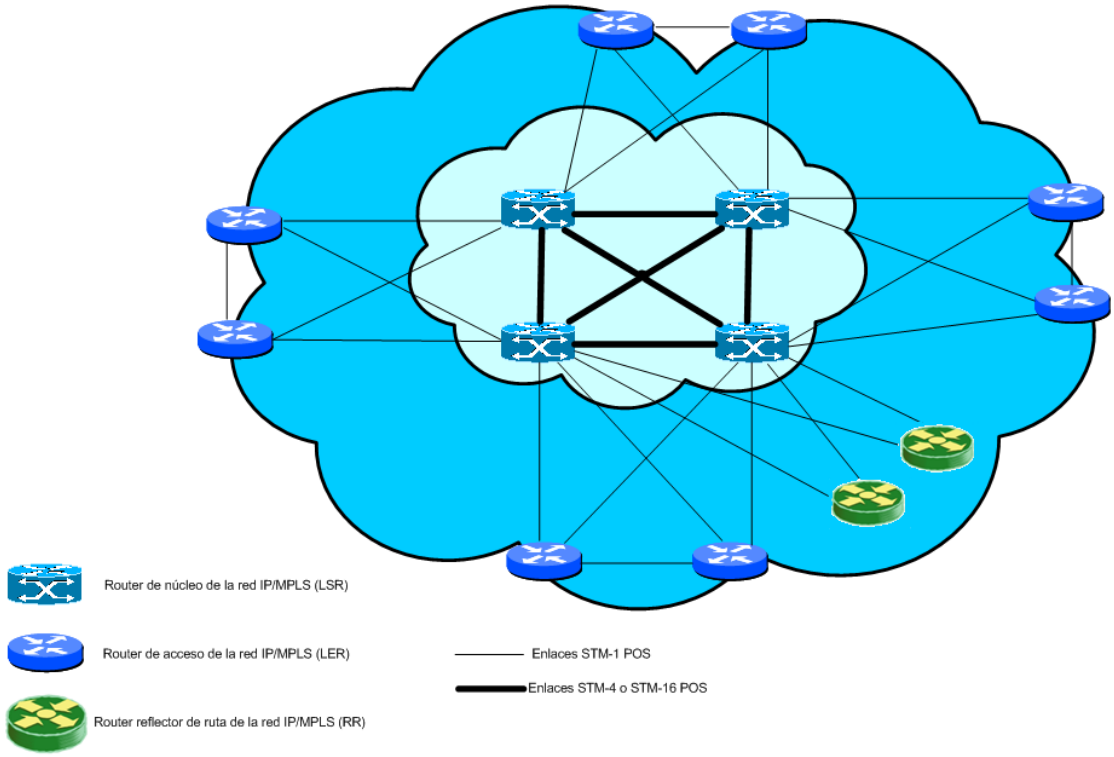


Figura 6.4.8 Esquema de los componentes del backbone del nivel de tránsito.Elaboración propia.

Cada uno de los dos routers que existen en los centros de acceso, se conecta a dos routers de tránsito diferentes por enlaces STM-1 y entre ellos la conexión también se produce mediante enlaces STM1 POS. Los routers de tránsito, acceso y conexión se conectan, a su vez, a cada uno de los dos reflectores de rutas que existen en la red; en el caso de existir conexión física, además de la lógica, ésta se realiza mediante enlaces STM1 POS.

La configuración del **protocolo BGP-4** en los routers que constituyen los centros de acceso, en los routers de conexión y en los reflectores de rutas, permite **conocer y propagar las direcciones** que se atienden en los diferentes centros de acceso que constituyen la red. El **encaminamiento de los paquetes** en el interior de la red se realiza **mediante la tecnología MPLS**, basado en un encaminamiento de paquetes en la red a través de la conmutación de etiquetas de longitud fija asignadas a cada uno de ellos. Previamente al encaminamiento de los paquetes en la red, se **definen caminos (LSPs, Label Switched Path)** en la misma. Para poder establecer estos caminos en el interior de la red los routers deben **conocer la topología**, por lo que es necesaria la configuración del **protocolo IS-IS** en todos los routers que componen el backbone de la red, tanto de los

centros de tránsito como de los centros de acceso. El establecimiento de caminos en la red se lleva a cabo siguiendo las pautas que marca el protocolo de **distribución de etiquetas LDP (Label Distribution Protocol).** La codificación de las etiquetas a las que se refieren estas RFCs se basa en la que impone la RFC 3032. Para una información mas especifica y detallada de los protocolos de routing empleados, consultar **en el documento memoria_anex.pdf apartado ANEXO19.**

6.4.4 Arquitectura detalla de la red del nivel de interconexión

Las conexiones con red nacional e internacional, Internet… se consideran **conexiones externas** y se realizarán a través de un **router de conexión (RC).** En todos los casos se utiliza el **protocolo BGP-4 para transferir la información de routing**. Las redes con las que interconecta la red **RIMA tendrán un sistema autónomo diferente**. En cada caso se utilizarán las técnicas de marcado y filtrado de direcciones. La red RIMA interconecta, entre otras, con las siguientes redes:

- Operadores nacionales (Ono, BT, Vodafone…)
- Red internacional de TIWS
- Operadores virtuales OMVs
- Red IRIS
- Internet

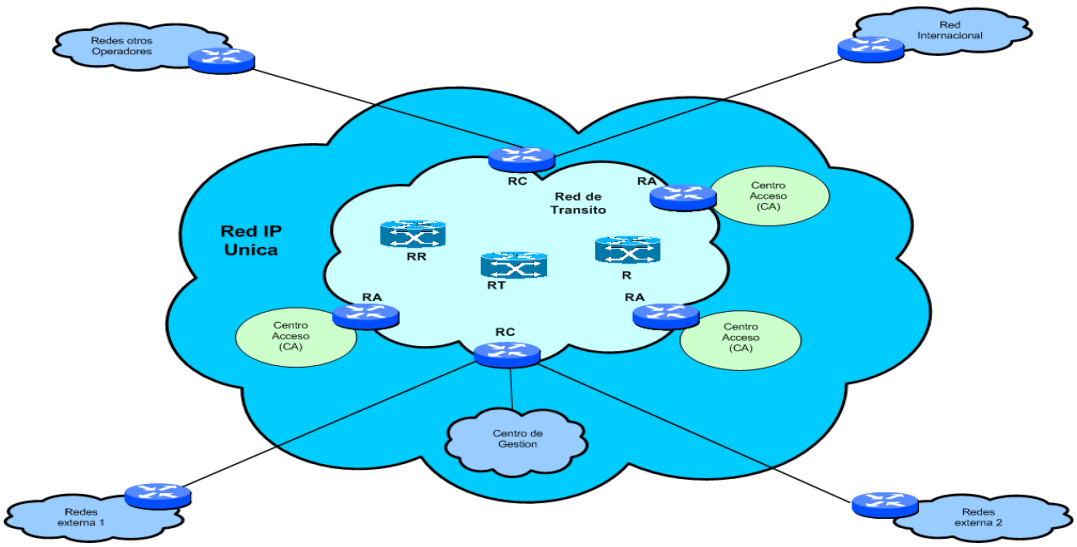


Figura 6.4.9 Esquema de interconexión de redes externas.Elaboración propia.

6.4.5 Transporte del tráfico IP

En función de la interfaz que exista en cada uno de los elementos que constituyen la red, el conjunto de protocolos a implementar variará.Para saber con detalle la pila de protocolo que intervienen en los diferentes interfaces de red **se puede consultar en el documento memoria_anex.pdf apartado ANEXO20.**

6.4.5.1 Calidad de Servicio

La calidad de Servicio en la Red IP Única de Telefónica se basa en la **arquitectura de Servicios Diferenciados (DiffServ)**. Para saber como es el octeto TOS para la calidad de servicio se puede consultar en el documento **memoria_anex.pdf apartado ANEXO21.**
En la RFC 2547, el IETF redefinió el "ToS octet" como "DiffServ Byte". En esta RFC a los **seis bits más significativos del ToS se les denomina DSCP**. Así pues, los tres bits más significativos del DSCP coinciden con la precedencia IP señalizada en el byte ToS. **En el acceso se usan 6 clases de las 8 posibles. En el núcleo se usan 4 de los 6 posibles.**

- **Clase de Servicio PLATA:** Orientada al tráfico Intranet del cliente y tiene prioridad normal.
- **Clase de Servicio ORO:** Orientada al tráfico Intranet del cliente de aplicaciones críticas. Tiene prioridad normal.
- **Clase de Servicio MULTIMEDIA:** Orientada al tráfico muy sensible al retardo y/o jitter (VoIP, multimedia, etc...). Tiene máxima Prioridad.
- **Clase de Servicio GESTIÓN:** Asociada al tráfico de gestión de los routers. No es una clase de servicio contratable por el cliente. Prioridad Alta
- **Clase de Servicio ROUTING**: Asociada al trafico de encaminamiento de los routers. Reserva un ancho de banda para el envío de las tablas de rutas. Prioridad alta
- **Clase de Servicio BRONCE:** Orientada al resto de tráfico que no ha sido clasificado en ninguna anterior, es decir, el tráfico por defecto. Tiene prioridad normal.

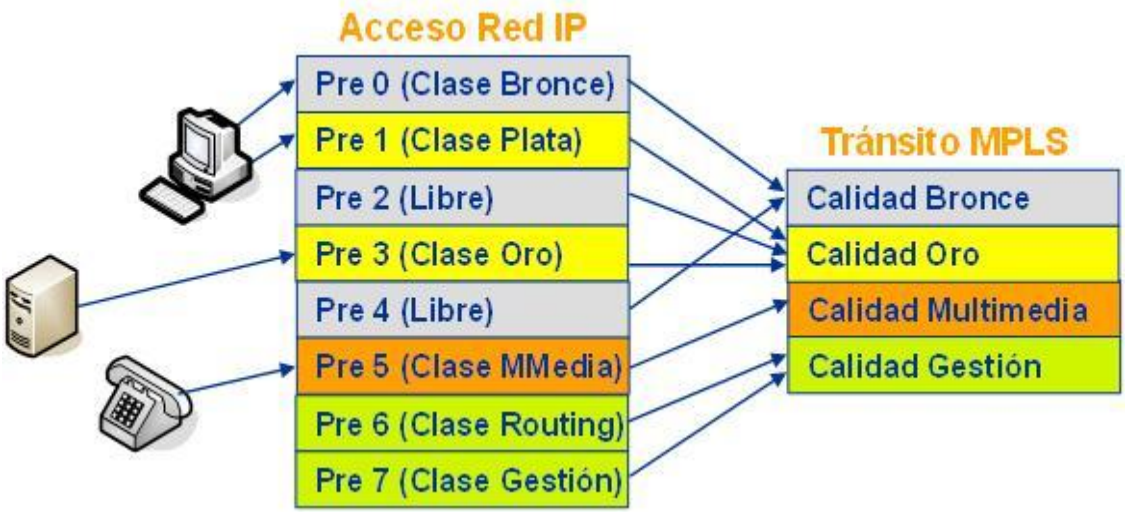


Figura 6.4.10 Tipos de clases de servicio en el acceso y en tránsito de la red IP Unica. Elaboración propia.

Para el tratamiento del tráfico en el tránsito de la red se emplea el MPLS EXP BIT de 3 bit. Para saber el formato de la cabecera MPLS se puede consultar en el documento **memoria_anex.pdf apartado ANEXO22.**

Se **pasaría de 6 a 4 clases de servicio en el tránsito de la red**. La implementación en el equipamiento de red se realiza por medio de colas diferenciadas y políticas de servicio. Tras el marcado de la calidad de servicio en el acceso, se realiza un **tratamiento diferente de cada tipo** tanto en los diversos equipos de la red:

- Los tráficos de **mayor calidad (Multimedia) se cursan de forma prioritaria para evitar retardo/jitter**.
- Los tráficos de **menor prioridad se sirven después de los prioritarios**, según su clase.
- En las colas se puede descartar tráfico en determinadas condiciones fijando un tamaño de buffer común asignado a cada clase:

  -Para tráfico Multimedia se imita la espera máxima para evitar altos valores de retardo/jitter.

  -Para otros tipos de tráfico, se realizan descartes en función del tamaño del buffer asignado.

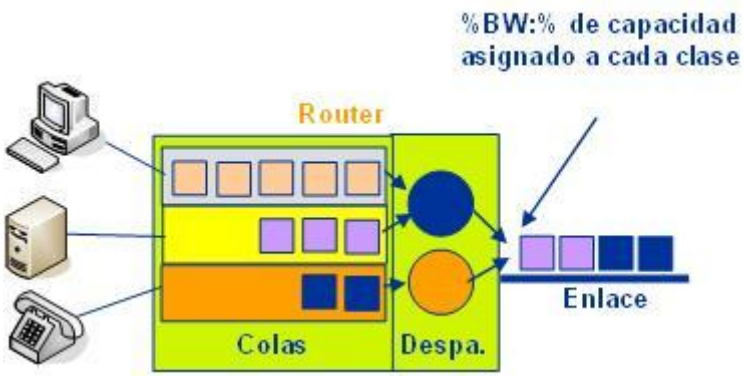


Figura 6.4.11 Esquema de encolado de tráfico según prioridades. Elaboración propia.

En los **routers de acceso (RA)** se implementa técnicas de **policía y CBWFQ**. Esta técnica CBWFQ consiste en dividir el ancho de banda disponible en tantos bloques como calidades de tráfico se vayan a gestionar y asignar a cada bloque el porcentaje de ancho de banda deseado. En los **routers de tránsito (RT) se implementa WRED**, donde WRED, consiste en el descarte de paquetes aleatorio en función el tráfico, consiguiendo suavizar la cantidad de tráfico cursado y evitar que la red llegue a la saturación.

6.4.6 RPVs IP en la red IP Única

Tal y como explique en la red UNO, para implementar **antiguamente soluciones de RPVs**, era necesario emplear líneas dedicadas y, sobre estas, configurar las distintas uniones con el resto de las sedes de la RPV. Estas uniones entre sedes se hacían de **forma estática** y utilizando para ello **generalmente Circuitos Virtuales Permanentes a través de la red UNO**. El problema que nos surgen con este tipo de redes es que **no son compatibles entre si los distintos tipos de acceso**, y para hacerlos compatibles, serían necesarios elementos especiales como pasarelas, etc… por eso las RPVs de la red UNO ya no se comercionalizan y las que existen **se migran a RPVs IP**. Debido a esto, surgió gran interés por las RPVs basadas en IP, ya que proporcionan conexiones basadas en redes como Internet mediante la formación de **TÚNELES IP**. Para saber mas sobre las RPVs

IP, en materia de conceptos, nomenclaturas y beneficios de las mismas consulta el documento **memoria_anex.pdf apartado ANEXO23.**

6.4.7 Servicios sobre la red IP Única

Una vez analizada la estructura de la red IP Única en la actualidad y explicado cómo se crean RPVs IP sobre la misma, estoy en condiciones de explicar los servicios para PYMES y grandes clientes que se ofertan en la actualidad que permiten la creación de RPVs IP o la conectividad con Internet utilizando la infraestructura de la red IP Única.

6.4.7.1 Servicio VPN-IP

6.4.7.1.1 Descripción del servicio

El Servicio VPN IP se define como un **servicio de Redes Privadas Virtuales, gestionado y definido sobre la red IP Única de Telefónica y basado en la tecnología MPLS (RFC 2547)**. Esta tecnología permite definir VPNs IP sobre una red IP pública, con las siguientes características:

- **El tráfico de cada VPN no se mezcla con el resto**, es decir, el tráfico perteneciente a una VPN va únicamente dirigido a delegaciones que pertenecen a esa VPN.
- **El direccionamiento de cada VPN es independiente respecto a las demás VPNs**. Es decir, cada VPN puede tener su propio esquema de direccionamiento (generalmente correspondiente a direcciones IP privadas), y además puede solaparse con el direccionamiento de otras VPNs.
- **Calidades de servicio**. El servicio dispone de varias calidades de servicio que permiten al cliente dar un tratamiento diferenciado a sus distintos tipos de tráfico.
- **Mecanismos de redundancia**. El servicio dispone de varias alternativas para proporcionar acceso redundante a la red MPLS y por tanto a la VPN IP.
- Privacidad y seguridad: las redes privadas virtuales basadas en MPLS **ofrecen el mismo nivel de privacidad y seguridad que las equivalentes a una VPN de nivel 2** mediante la limitación de distribución de rutas de una RPV a únicamente aquellos routers que son miembros de esa RPV.

- **Facilidad de provisión**. Debido a la topología totalmente mallada de VPN IP proporcionada por la red MPLS, se pueden añadir sitios a las intranets sin más que dar de alta la correspondiente conexión.
- Es posible **utilizar cifrado IPSec** entre distintas sucursales, determinadas por el cliente.
- Es **un servicio gestionado** que incluye cambios en las configuraciones de los routers por parte de Telefónica.

6.4.7.1.2 Modalidades de Acceso

El acceso a la Red IP Única, que constituye el núcleo de la VPN del cliente, dependerá de los requerimientos del cliente fundamentalmente en lo referente a la necesidad de coexistencia de diferentes servicios en el mismo acceso y al caudal IP que el cliente debe contratar para soportar el tráfico a transmitir/enviar desde cada una de sus delegaciones. Se contemplan dentro del servicio VPN IP los siguientes mecanismos de acceso:

- Accesos a través de la Red UNO/Multiservicio.
- Accesos directos mediante circuitos Pto a Pto (IP Nativo).
- Accesos de nueva generación ADSL2+,VDSL2 y FTTH.
- Accesos ADSL empleando el servicio GigADSL.
- Accesos conmutados.
- Accesos móviles.

Los esquemas de red de las difententes modalidades de acceso asi como su explicación detallada se puede consultar en el documento **memoria_anex.pdf apartado ANEXO24.**

6.4.7.1.3 Acceso a Internet

En el servicio **existe la posibilidad de que todas las sedes VPN-IP tengan salida a Internet** mediante el servicio DataInternet/DIBA ofrecido por Telefónica y que explicare más adelante. Existen dos posibles escenarios, en los cuales es posible denegar el acceso a Internet a determinadas oficinas pertenecientes a la misma VPN definidas por el cliente.

6.4.7.1.3.1 Acceso a Internet no Integrado en Red (Caudal IP)

Si el cliente dispone de una **salida a Internet** en alguna de las **sedes** (en general una sede a la que podríamos considerar **como central**), ésta **puede anunciar la ruta por defecto** a través de la VPN para que el resto de sedes hagan salida a través de dicha conexión**, pudiendo hacer NAT** (Networkt Address Translation) para traducir de las direcciones privadas de las sedes a la pública de salida a Internet si fuera necesario. En este caso la sede central necesitará emplear un routing basado en RIP bidireccional o BGP, ya que la ruta estática por defecto en el router deberá apuntar hacia donde se ofrezca la salida a Internet.

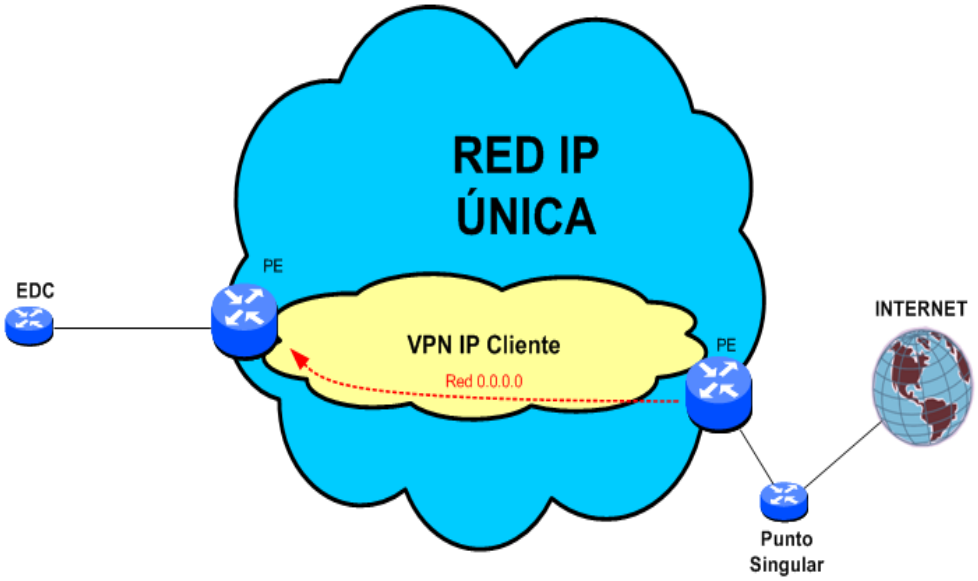


Figura 6.4.12 Esquema de salida a Internet desde una sede a través de una sede central. Elaboración propia.

6.4.7.1.3.2 Acceso a Internet Integrado en Red (Caudal Agregado)

En este escenario se proporciona una **salida a través de un punto de interconexión a Internet común** para todos los clientes con servicio VPN-IP. Este **punto de interconexión está formado por dos equipos Shasta, uno en Madrid y otro en Barcelona**, que hacen Backup el uno del otro. Para realizar esta salida, el cliente contratará un servicio Datainternet con caudal agregado, que le dará una conexión entre su VPN-IP y los Shasta. A través de dicha conexión se cursará su tráfico hacia Internet.

Para hacer esta salida agregada, el cliente **contrata una conexión de su VPN contra el Shasta**, exactamente igual que si se tratase de una sede más dentro de la red del cliente. Lo único que hará será **inyectar la ruta por defecto dentro de la VPN**, de tal manera que el

resto de las sedes cursen el tráfico de internet por esta conexión. Posteriormente, el Shasta encaminará este tráfico y el de todas las demás VPNs con salida a Internet.

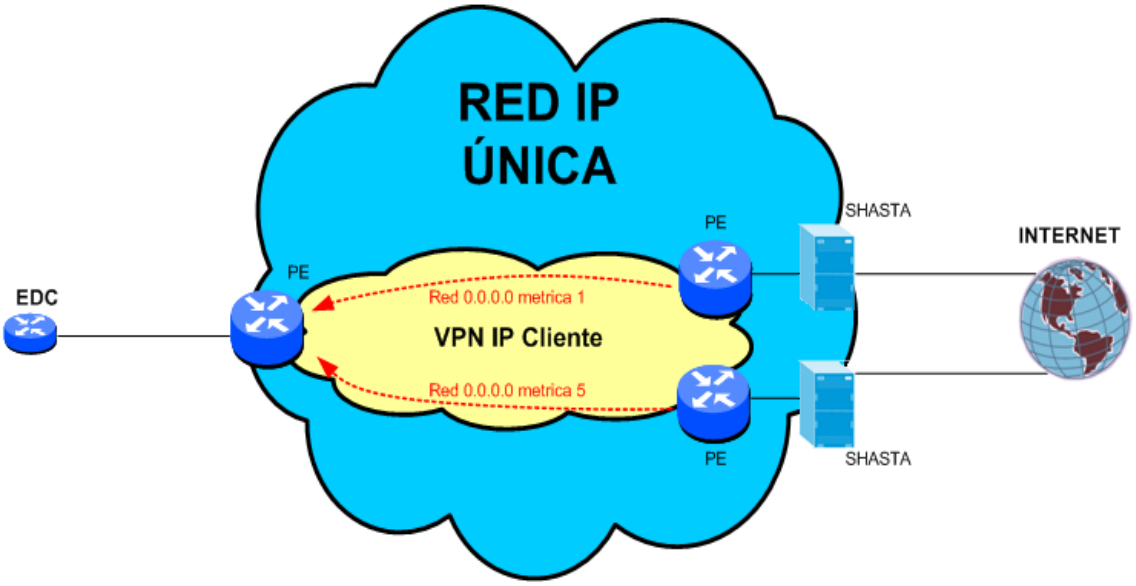


Figura 6.4.13 Esquema de salida a Internet integrado en red a través de los Shastas.Elaboración propia.

6.4.7.1.4 Calidades de Servicio

El servicio VPN-IP permite al cliente contratar **calidades de servicio** que permiten al **cliente garantizar caudales para aplicaciones sensibles y priorizar su tráfico** multimedia dentro de la VPN. Estas calidades de servicio **se den a lo largo de todo el trayecto** (entre origen y destino), aunque, realmente, donde más sensible es, es en los puntos de acceso del cliente (las líneas físicas donde se conecta el cliente a la red).

Para poder garantizar estas calidades, se definen cuatro clases de servicio **(Multimedia, Oro, Plata y Bronce),** dependiendo del tipo de tráfico y que ya se explicó anteriormente en el punto 7.4.11. Estas clases de servicio deben configurarse en todo el trayecto, tanto en PEs como en Ps y sólo entran en funcionamiento en caso de saturación, con lo que las zonas críticas son las conexiones con el cliente.

6.4.7.1.5 Mecanismos de redundancia de accesos y respaldos

Para **aumentar la disponibilidad** de un punto (por ejemplo, el CPD), se puede contratar una **segunda línea** con un funcionamiento de reparto de carga, es decir, cada una de ellas cursa el 50% del tráfico contratado, o en modo backup (la línea de backup se activará cuando caiga la línea principal y cursará el 100% del tráfico contratado) También existe la posibilidad de tener un **segundo EDC** que redunda al principal, funcionando en modo backup o reparto de carga.

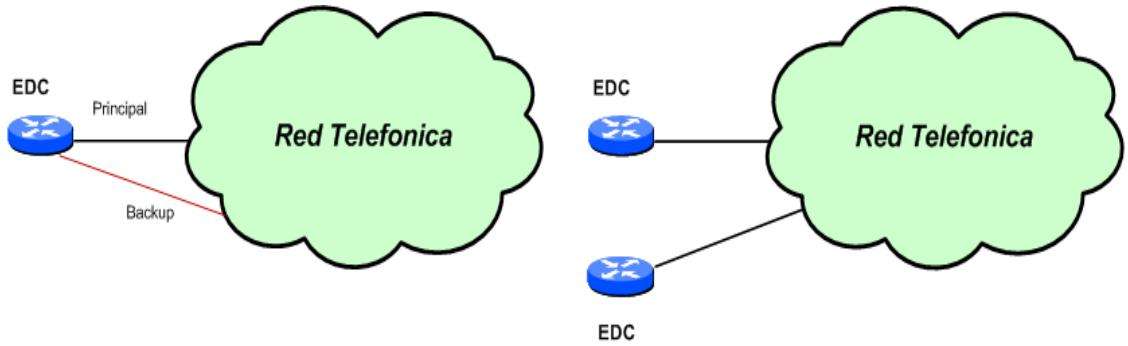


Figura 6.4.14 Esquema de redundancia de líneas y de edcs. Elaboración propia.

Los mecanismos de respaldo, también denominados backup, para el servicio VPN-IP siempre cubren el acceso. Esto es, las distintas soluciones de backup protegen a las sucursales ante:

- Caída de la línea principal de acceso a la VPN-IP.
- Caída del nodo de red empleado como punto de acceso por parte de una sucursal de la VPN-IP.

A la hora de implementar **soluciones de backup**, existen tres alternativas:

- Líneas fijas **asimétricas (ADSL).**
- Respaldos basados en **RDSI**.
- Respaldos **móviles (GPRS/UMTS).**

6.4.7.1.6 Funcionalidades de valor añadido

El servicio VPN-IP permite contratar facilidades adicionales que permita a los clientes cubrir sus necesidades y expectativas.

6.4.7.1.6.1 Facilidad de cifrado IPSEC

La posibilidad de cifrar datos responde a la necesidad de algunos clientes de garantizar la confidencialidad, integridad y autenticidad de los datos que intercambian entre sus distintas sedes. El **cifrado** que se va a proporcionar es **IPSEC en modo túnel con secreto compartido y 3DES** que permitirá asegurar que todo el tráfico enviado por este túnel no ha sufrido ningún tipo de alteración, no ha sido leído por un tercero y, lo que es más importante, el tráfico viene de su emisor original. Para obtener una información mas exhaustiva del protocolo IPSEC consultar el documento **memoria_anex.pdf apartado ANEXO25.**

6.4.7.1.6.2 Facilidad de Multivrf

La facilidad de **Multi-VRF** permite **definir en los EDCs diferentes "routers virtuales"** que den servicio a **diferentes VPNs** de uno o más clientes. Cada uno de los interfaces lógicos del router se asociará a uno de los planos de **routing definidos en el EDC** y por tanto a todos los efectos será de uso exclusivo de una determinada VPN. La comunicación entre las VPNs definidas en el PE y las VPNs definidas en el EDC, se realizaran definiendo al menos un Circuito virtual F.R o ATM por VPN o mediante accesos físicos separados, en cuyo caso pueden ser ADSL, FR, ATM. La conectividad de cada una de las VPNs con la LAN de cliente, podrá ser mediante interfaces Ethernet/FastEthernet físicos dedicados o SubInterfaces 802.1q, se introduce por tanto el soporte de VLANes.

6.4.7.1.6.3 Facilidad Telefonía IP (ToIP)

Sobre la **misma infraestructura de datos se puede transmitir voz** garantizando los niveles máximos de convergencia entre voz y datos **gracias a las calidades de servicio** y proporcionando una integración de funcionalidades en los EDC's. Los elementos que están dentro del ámbito de gestión del servicio VPN IP son el EDC, y el Gateway, quedando los Teléfonos IP y el Gestor de Llamadas (encargado de gestionar la conmutación de llamadas, entre otras funciones) dentro **del servicio Ibercom IP** que explicare más adelante.

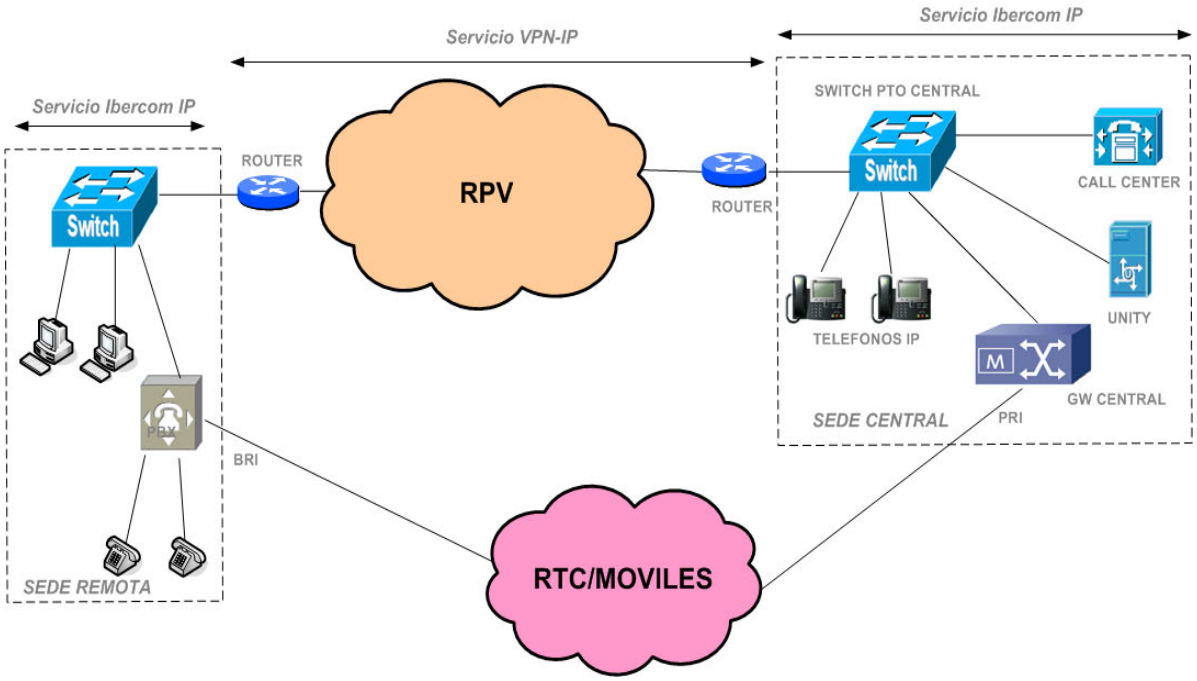


Figura 6.4.15 Facilidad de ToIP sobre el servicio VPN-IP.Elaboración propia.

6.4.7.1.6.4 Facilidad de Soporte de otros Protocolos

Las facilidades de XoT y DLSW en los EDCs del servicio VPN IP permiten a los protocolos tradicionales, como son X.25, SNA, ser transportados de forma eficiente a través de una red IP.

1) Soporte **XOT**: Permite conectar **dispositivos X.25 al EDC** del servicio y encapsularlo en IP. Especialmente útil en entornos bancarios para la conexión de cajeros. No aplica para accesos móviles.

2) Soporte **DLSW**: Permite el **transporte** a través de una red IP de los protocolos **SNA y NetBIOS (IBM**). Especialmente interesante en entornos bancarios para la conexión de oficinas al CPD.No aplica para accesos móviles

6.4.7.2 Servicio Macrolan

6.4.7.2.1 Descripción del servicio

MacroLAN es un **servicio gestionado** de **Red Privada Virtual** en la que se hace **routing del tráfico IP** del cliente entre distintas sedes. De forma adicional, la facilidad de Transporte Ethernet del servicio permite también el **transporte transparente de tramas Ethernet** entre diferentes sedes del mismo cliente de forma similar a como si las diferentes sedes estuviesen conectadas mediante una red de área local. MacroLAN se apoya sobre la **infraestructura que constituye las redes Ethernet de Telefónica** de España (MAN) como medio de acceso a la red IP Única, la cual sirve de infraestructura que permite tanto la interconexión de los emplazamientos de un cliente en un mismo área provincial como la conexión con la red IP Única que proporciona la comunicación entre dependencias del cliente a nivel nacional. **La cobertura del servicio MacroLAN es, por tanto, nacional**. Sin embargo, para el servicio se distingue dos ámbitos:

- Ámbito **provincial**, en el cual el servicio **se apoya**, principalmente, en la **infraestructura de la MAN.**
- Ámbito **nacional**, en el cual, además de la MAN, se utiliza la infraestructura de la **red IP Única**.

El objetivo principal es mantener al menos el mismo nivel de privacidad que se tiene en las RPVs tradicionales, es decir, proporcionar una protección equivalente a la de un circuito Frame Relay o ATM. La **tecnología utilizada para garantizar el aislamiento de tráfico** entre clientes es distinta en función del entorno que se considere:

- En entorno metropolitano/provincial (cobertura MAN) se utilizan bien tecnologías de LAN virtual (**VLAN según IEEE 802.1Q) o de VPLS**.
- En entorno nacional se implementan **RPVs IP** según la **RFC 2547 bis**.

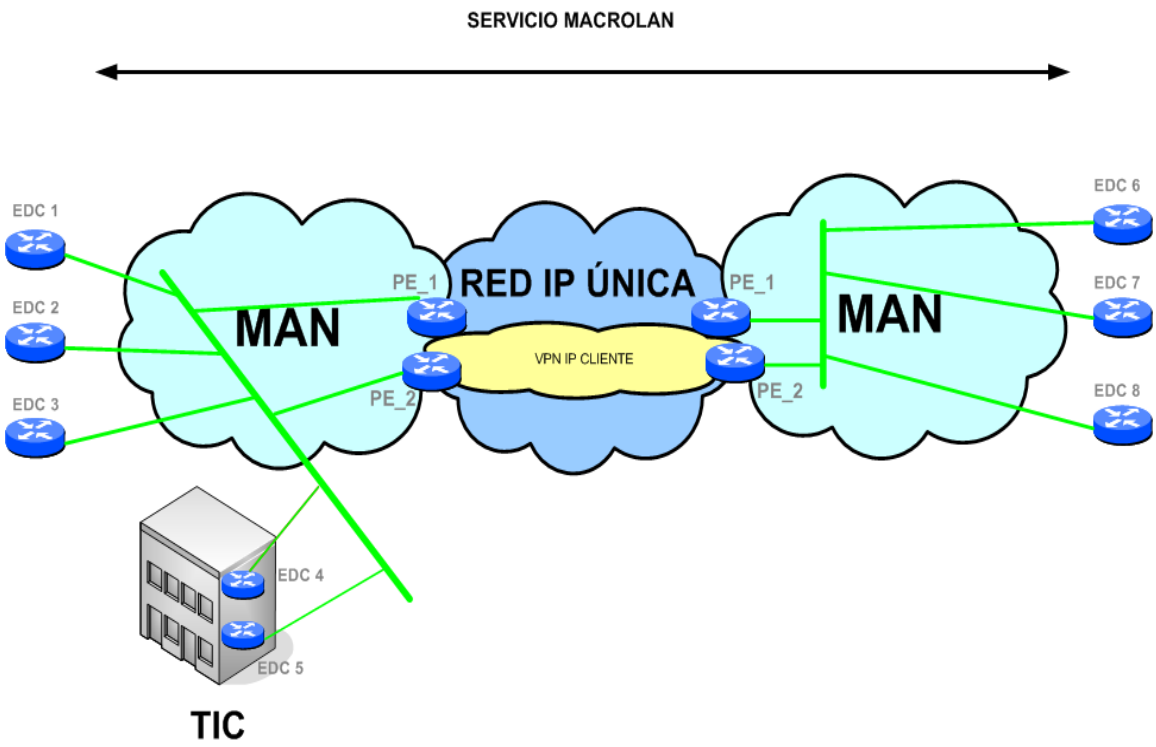


Figura 6.4.16 Esquema general del servicio Macrolan.Elaboración propia.

6.4.7.2.2 Arquitectura lógica del servicio

MacroLAN es un servicio de RPV en el que:

- Parte de la infraestructura sobre la que se sustenta es exclusiva de un cliente (línea de acceso a la MAN).
- Otra parte es compartida por varios clientes (la red MAN y la red IP Única).

Tecnologías utilizadas para separar tráfico entre clientes:

- VLAN en entorno metropolitano (IEEE 802.1Q).
- MPLS IP VPN a nivel nacional (RFC 2547).

6.4.7.2.2.1 Tipos de vlanes

Como el servicio Macrolan emplea vlanes para separa el tráfico entre clientes, existen **3 tipos de vlanes en función del ámbito de la comunicación** entre delegaciones:

1) **Vlan metropolitana**: Permite comunicar a los EDC dentro de la misma provincia sin necesidad de utilizar la red IP Única y solo haciendo uso de la MAN de la provincia.

2) **Vlan nacional:** Permite comunicar con EDCs ubicados en una MAN remota, es decir, proporcionar una comunicación nacional entre MAN provinciales haciendo uso de la red IP Única. En los PEs, esta vlan se mapea a la "VPN IP" del cliente. Adicionalmente permite dicha vlan, la conectividad con EDCs ubicados en el TIC (Telefónica Internet Center), que es un emplazamiento que proporciona Telefonica a los clientes como si se tratase de una delegación mas de los mismos.
3) **Vlan TIC Nacional:** Permite comunicar un EDC alojado en el TIC con otros ubicados en una MAN remota, es decir, proporciona una comunicación nacional entre EDCs que estén ubicados en otras MAN. En los PEs, esta vlan se mapea a la "VPN IP" del cliente.

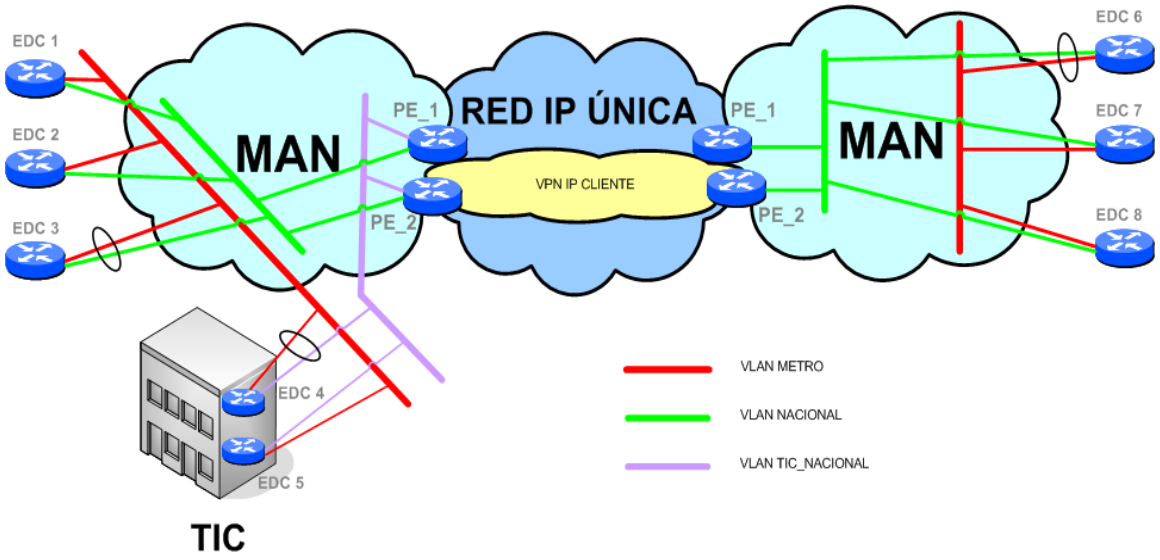


Figura 6.4.17 Esquema de distribución de vlanes en el servicio Macrolan.Elaboración propia.

6.4.7.2.2.2 Tipos de escenarios

En función de la distribución de las delegaciones de un cliente y el número de ellas, podemos establecer unos escenarios:

- **Cliente con N sedes en la misma provincia.**
- **Cliente con N sedes en la provincia A y una sede en la provincia B.**
- **Cliente con N sedes en la provincia A y N sedes en la provincia B.**
- **Cliente con N sedes en la provincia A, N sedes en la provincia B y 1 sede en el TIC.**

Para conocer los esquemas de red y caracteristicas de los anteriores escenario ademas de saber los interfaces y velocidades empleadas para conectarse a la MAN, se puede consultar **en el documento memoria_anex.pdf apartado ANEXO26.**

6.4.7.2.3 Caudales Macrolan

En el ámbito del servicio MacroLAN se distinguen los siguientes tipos de caudales:

- Caudal **Metro**
- Caudal **Nacional Agregado**
- Caudal **Nacional Exclusivo**
- Caudal **TIC Agregado**
- Caudal **TIC Exclusivo**

Para obtener información sobre cada uno de los caudales anteriores, consultar el documento **memoria_anex.pdf apartado ANEXO27.**

En MacroLAN, hay definidas 3 clases de servicios: **Multimedia, Oro y Plata**. Cada uno de los caudales arriba indicados, se compone realmente de la suma de los caudales correspondientes para cada clase de servicio. El cliente contrata en realidad un caudal determinado para cada clase de servicio.

6.4.7.2.4 Escenarios de conexión con la MAN

Dependiendo de las necesidades del cliente y la necesidad de búsqueda de fiabilidad, el servicio Macrolan ofrece los siguientes escenarios:

- Un EDC con acceso único.
- Un EDC con acceso doble.
- Doble EDC en reparto de carga.
- Doble EDC en modo backup o respado.

Para saber los esquemas y funcionamiento de las topologias anteriores, consultar el documento **memoria_anex.pdf apartado ANEXO28.**

6.4.7.2.5 Calidad de Servicio (QoS)

MacroLAN define **tres clases de servicio** contratables por el cliente: **Plata, Oro y Multimedia**; más una clase adicional para el tráfico de gestión de los EDCs, que es transparente para el cliente. Es el mismo concepto que en el servicio VPN-IP.

6.4.7.2.6 Facilidades del servicio

A continuación se enumeran cada una de las facilidades adicionales del servicio:

1) Alojamiento de oficina del cliente en el TIC

Esta oficina se trata como una **sede** más de la red privada virtual del cliente **pero ubicada en dependencias de Telefónica.**

2) Transporte Ethernet

Permite el transporte transparente **de tráfico Ethernet entre EDCs**, siendo transparente a protocolos de nivel 3 y superiores. Es una facilidad de conectividad de nivel 2.

3) Transporte de ToIP (Ibercom IP)

Sobre la **misma infraestructura de datos se puede transmitir voz** garantizando los niveles máximos de convergencia entre voz y datos, y proporcionando una integración de funcionalidades en los EDC's.Los elementos que están dentro del ámbito de gestión del servicio Macrolan son el EDC, y el Gateway, quedando los Teléfonos IP y el Gestor de Llamadas (encargado de gestionar la conmutación de llamadas, entre otras funciones) dentro del servicio Ibercom IP.

4) Redirección "Plus"

Permite, bajo demanda explícita del cliente, que el **tráfico enviado normalmente hacia un punto central "A" pase a cursarse hacia un punto central "B"**.Ambas sedes deben pertenecer al servicio MacroLAN, pudiendo o no estar ubicados en el mismo área metropolitana/provincial.

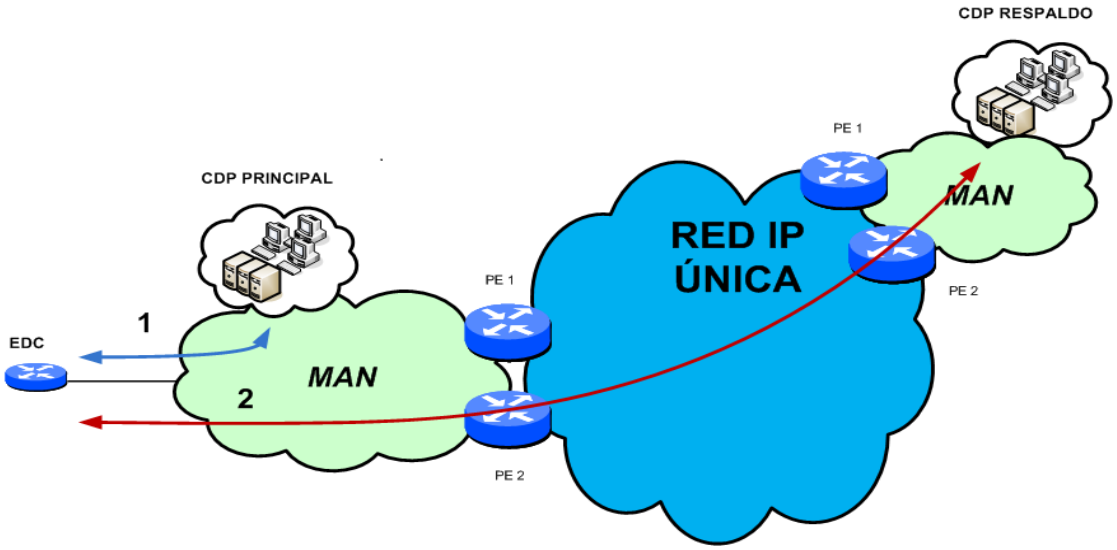


Figura 6.4.18 Esquema de la facilidad de Redirección Plus.Elaboración propia.

5) Cifrado del tráfico IPSec

La facilidad de cifrado, es el **mismo concepto explicado para el servicio VPN-IP** en el punto 7.4.11.1.6.1 y permite la encriptación y autenticación del tráfico de cliente cursado entre sedes del mismo mediante IPSec. El cliente define, mediante los criterios disponibles, qué tipo de tráfico entre sus sedes quiere que sea cifrado para su envío. La única restricción es que **el tráfico Multimedia y el destinado a Internet no son susceptibles de ser cifrado**. La opción estándar es con túneles estáticos.

6.4.7.3 Servicio Datainternet

6.4.7.3.1 Descripción del servicio

El servicio **DataInternet** se define como un **servicio de conexión a Internet** sin restricciones a través de la **Red UNO** de **TdE desde pequeñas ubicaciones, hasta corporaciones con grandes redes privadas.** El servicio ofrece diferentes **tecnologías de acceso**:

- **Frame-Relay**.
- **ATM**.
- **ADSL**.
- **IP Nativo**.

- **Fibra Óptica** (Modalidad Datainternet Banda Ancha o DIBA).

Para este ultimo acceso, se basa en el uso de Redes de Área Metropolitana (MAN) de Banda Ancha en lugar de la red UNO para ofrecer la salida a Internet. Datainternet proporciona al Cliente facilidades adicionales como:

- Informes de uso de caudal,
- Parámetros de calidad de red (retardos, pérdidas y disponibilidad de los accesos),
- Posibilidad de facturación por uso, plana o mixta.
- Permite Caudales Asimétricos siempre que se cumpla: **Caudal Ascendente ≥ Caudal Descendente**
- Perfecta integración con los servicios de RPV de TDE.
- Opciones de alta disponibilidad.
- Solución integral gestionada por TDE.
- Opciones de Seguridad ofrecidas desde la propia red.
- Compromiso de Calidad de Servicio a través de SLA´s.

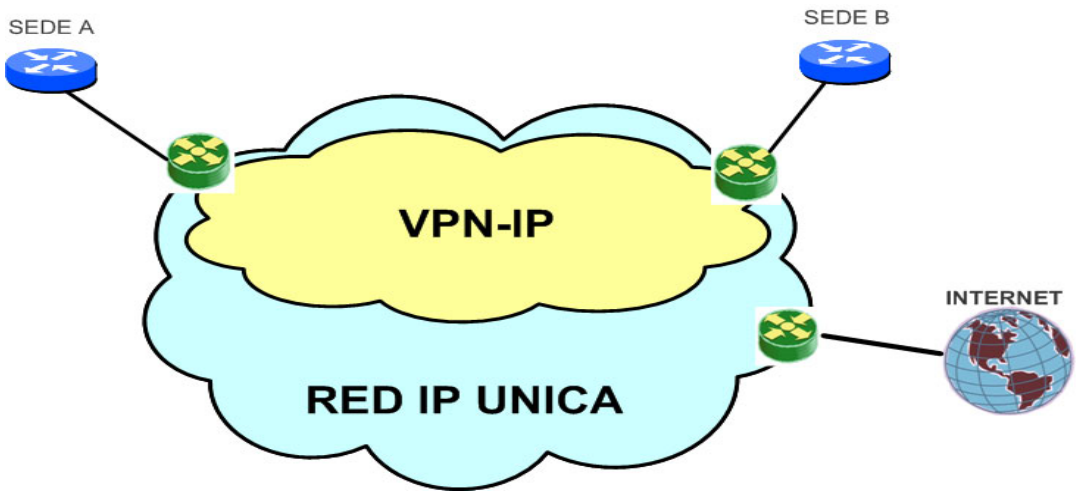


Figura 6.4.19 Esquema general del servicio Datainternet.Elaboración propia.

6.4.7.3.2 Modalidades de acceso

Los accesos empleados para el servicio Datainternet o Datainternet Banda Ancha (DIBA) tienen que ser capaces de unir la sede del cliente con red IP Única para proporcionar la salida a Internet mediante los shastas. Para realizar esta unión se pueden emplear tres métodos:

1) Empleando la Red UNO: Mediante Circuitos Virtuales Permanentes se creará la conexión de Nivel 2 entre el EDC y la Red IP Única. Empleado en Frame-Relay, ATM y ADSL.

2) Empleando la Red MAN: Utilizando las Redes MAN se consigue crear la unión entre los EDCs y el Router de Acceso de Red IP Única. Para cada una de las conexiones se empleará una VLAN distinta. Se emplea en Datainternet Banda Ancha (DIBA). Para este escenario es necesaria la convivencia con el servicio Macrolan.

3) Empleando un Acceso Directo a la Red IP Única.- Es decir, un enlace directo a nivel 1 (bajo la red Ibermic) entre el domicilio de cliente y Red IP Única.

La explicación detallada de los tres escenarios anteriormente comentados se puede consultar en el documento **memoria_anex.pdf apartado ANEXO29.**

6.4.7.3.3 Caudales de Internet

Partiendo de la premisa anteriormente comentada de que el caudal ascendente debe ser mayor o igual que el descendente y dependiendo del tipo de acceso existen diferentes caudales y modalidades del servicio DataInternet. Cada uno de los tipos de accesos, modalidades se encuentran explicados en el documento **memoria_anex.pdf apartado ANEXO30.**

6.4.7.3.4 Facilidades del servicio

6.4.7.3.4.1 Facturación flexible

DataInternet dispone de **tres modalidades de facturación** del servicio, en función del uso que el cliente hace del caudal contratado:

- La **facturación plana** es independiente del consumo que se realiza por parte del cliente. Es la opción que se adapta a clientes con patrones de consumo conocidos y constantes.
- La **facturación por uso** se realiza en función del consumo por parte del cliente. Es óptima para clientes que no conocen a priori el caudal que van a consumir o para aquellos con necesidades muy variables. Permite configurar un límite superior que garantiza una facturación máxima.

- La modalidad de **facturación mixta** permite facturar una parte del tráfico bajo modalidad plana y el exceso mediante facturación por uso.

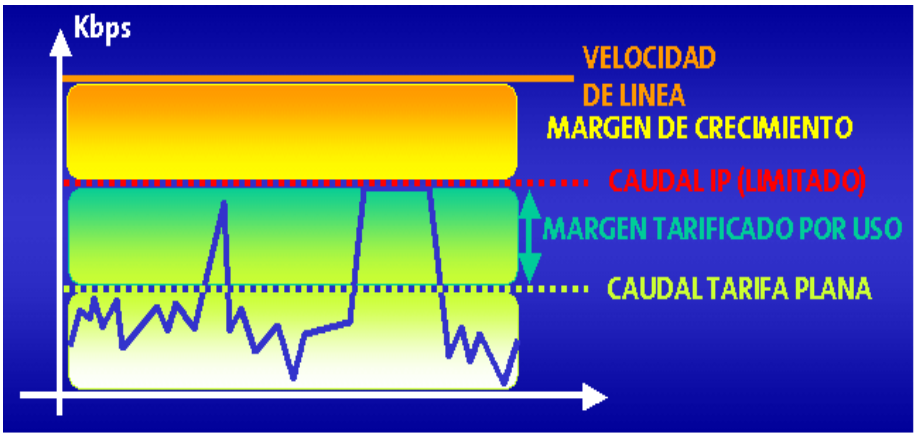


Figura 6.4.20 Gráfico de tarificación del servicio Datainternet

6.4.7.3.4.2 Alta fiabilidad y redundancia

El servicio DataInternet la posibilidad de **tener por duplicado** cualquiera de los elementos fundamentales del servicio, es decir:

- **Doble EDC.**
- Doble **línea de acceso** (implica 2 conexiones).
- **Doble conexión** (CVP FR o ATM o VLAN) **sobre la misma línea de acceso**.

Siempre que se opte por alguna opción de redundancia, las conexiones finalizarán en elementos de Red distintos. Es decir, no se le da la posibilidad al Cliente de escoger si la conexión termina en el mismo o distinto elemento de Red.

6.4.7.3.4.3 Funcionalidad NAT/PAT

Para la comunicación con Internet desde/hacia direcciones privadas de Cliente, es necesario hacer una **traslación del direccionamiento privado a direccionamiento público** y viceversa. Esta traslación puede ser exclusivamente **de dirección (NAT Network Address Translation)** o **de dirección y puerto (PAT Port Address Translation).**La funcionalidad de NAT/PAT se implementará en el EDC o en red sobre los Shasta.

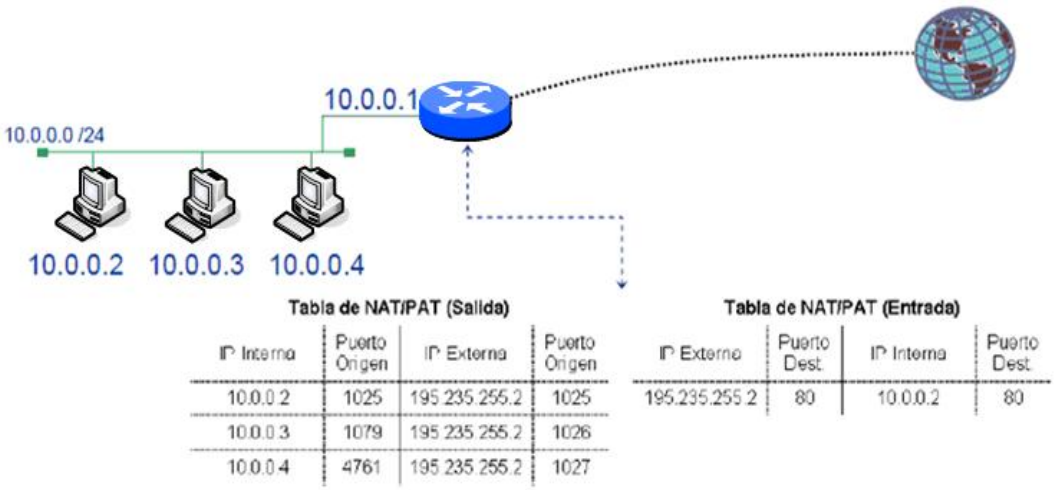


Figura 6.4.21 Esquema de la funcionalidad de NAT/PAT para DataInternet. Elaboración propia.

6.4.7.3.4.4 Gestión de direcciones IP

Telefónica España realiza las **tareas de registro y asignación de direcciones IP públicas** ante los organismos competentes. En el proceso de provisión de red se recogerá información de las direcciones IP del Cliente sólo con el objetivo de configurar el router de acceso de red IP.

6.4.7.3.4.5 Gestión de nombres de dominio y servicio DNS

El servicio DataInternet ofrece las **dos facilidades** fundamentales siguientes:

- **Gestión de Nombres de Dominio:** Telefónica España ejecuta, en nombre del Cliente, las tareas de registro de nuevos nombres de dominio ante los organismos competentes, solicitando al Cliente los datos necesarios para la tramitación del dominio.
- **Servicio de Resolución de Nombres (DNS):** El servicio DNS permite, por un lado, la resolución de URL's a los usuarios que acceden a Internet desde las redes del Cliente. Por otro lado, el servicio DNS hace público, al resto de Internet, los nombres de dominio de máquinas localizadas en las redes del Cliente.

6.4.7.3.4.6 Filtrado de contenidos

El servicio de Filtrado de Contenidos consiste en hacer pasar por un proxy las peticiones http de los usuarios de las distintas empresas. Cuando el usuario final realice una petición http por medio de un navegador, esta petición llegará al Shasta y este se encargará de redirigirla hacia una de las Unidades de Filtrado. La Unidad de Filtrado enviará una solicitud de autenticación al navegador del usuario y éste le mostrará una ventana solicitando un identificador de usuario y una password. Este identificador será utilizado por el Servicio de Filtrado (SF) para asignarle un perfil al usuario, y de esta forma, controlar los accesos que realice vía web. Si el Cliente cuenta con un Servidor Proxy en su red, se podrá configurar dicho servidor de manera que sea él mismo el que realice el proceso de autenticación contra la Unidad de Filtrado. De esta manera, no se solicitará autenticación a los usuarios finales. El flujo de operaciones que se realizan en el SF es el siguiente:

1. El **SF comprueba si la dirección URL** de la página solicitada se encuentra en las **listas predefinidas**.
2. En caso de que esté, dependiendo de su clasificación y del perfil asociado al usuario, su contenido será mostrado o no.
3. Si no se encuentra en las listas, su contenido es analizado por el motor de análisis.
4. Si el motor de análisis **establece que la página es de contenido inadecuado el usuario es avisado y se le evita el acceso. Si no, la página es mostrada.**

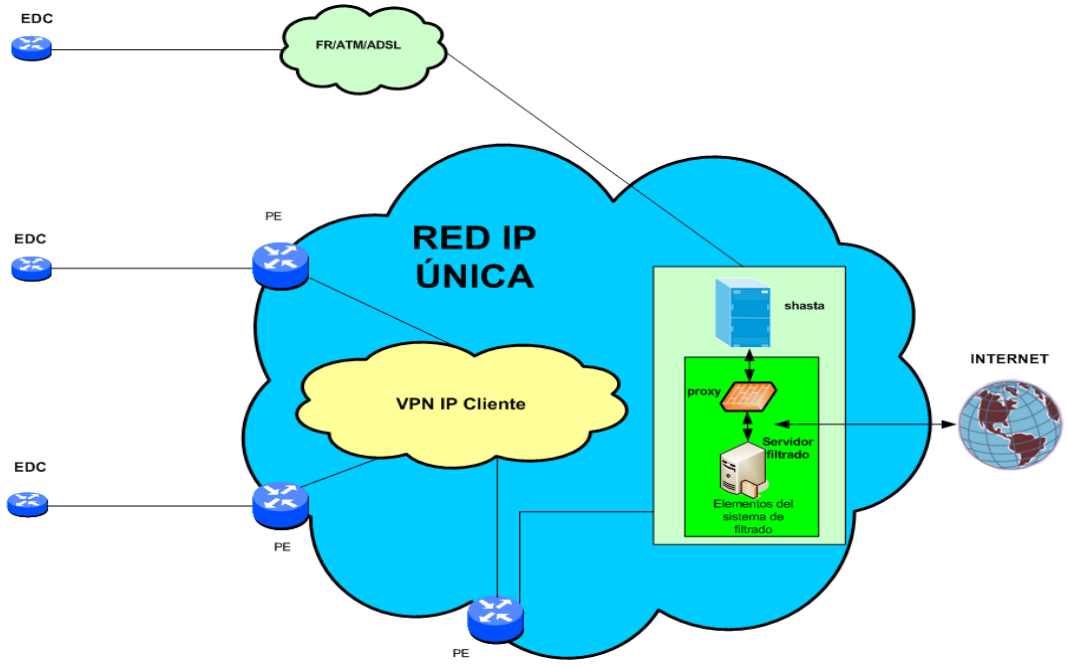


Figura 6.4.22 Esquema de la funcionalidad de filtrado de contenidos.Elaboración propia.

6.4.7.3.4.7 Seguridad: Firewall en red

La funcionalidad de firewall en red consiste en disponer de un **servicio de cortafuegos en la red** de acceso a Internet, en lugar de situar dicho firewall en la red del Cliente. Esta solución ofrece la ventaja de que los Clientes pueden **delegar en este firewall la política de seguridad** para el acceso a Internet, dedicándose ellos a la gestión de la política de seguridad interna. El Shasta es quien realiza la función de FW.

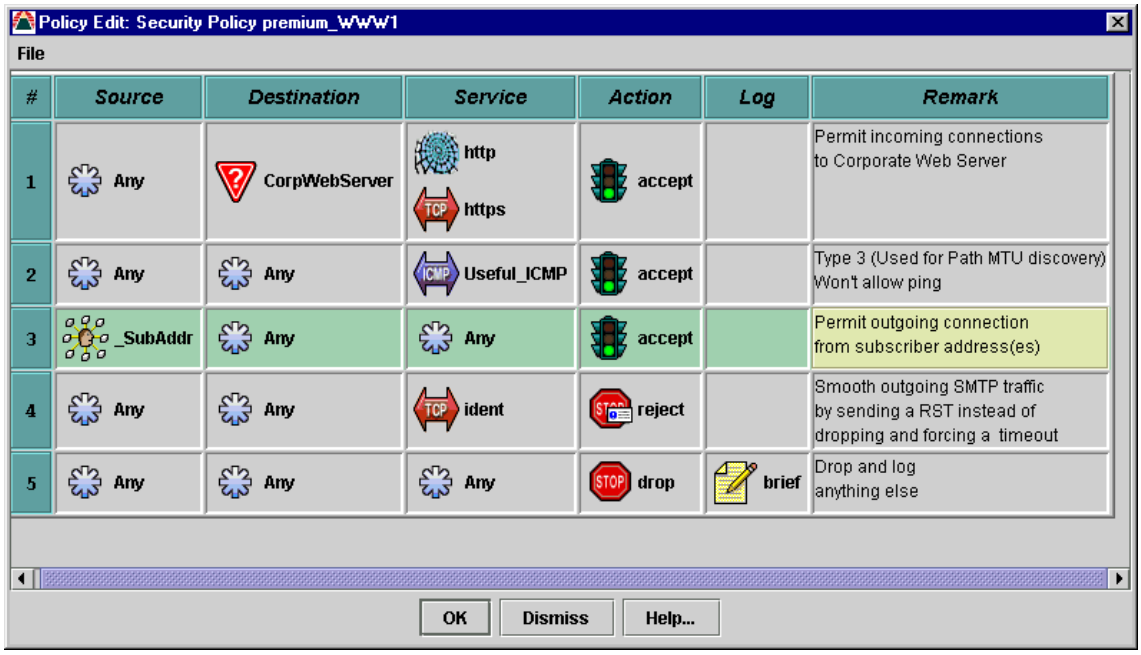


Figura 6.4.23 Ejemplo de reglas de FW para filtrar el tráfico

Además, el firewall del equipo Shasta está basado en la arquitectura **Stateful Firewall**. Esta técnica se basa en **examinar todos los paquetes**, tanto los entrantes como los salientes, aplicando sobre ellos la misma política de seguridad. Las reglas de la **política de seguridad se aplican sobre conexiones IP**, no sobre cada uno de los paquetes que circulan a través del enlace.

6.4.7.3.4.8 Conectividad IPv6

El DataInternet permite la **conectividad IPv6** como funcionalidad. Para proporcionar dicha conectividad TdE dispone de una **pasarela que interconectara la actual red IPv4 con la red IPv6**. La solución adoptada para dar conectividad IPv6 se basa en el uso de **Túneles Manuales Router a Router IPv6/IPv4**. Estos túneles, que se realizaran a través

de la conexión IPv4 del cliente, conectaran de manera lógica el Router de cliente y la Pasarela.

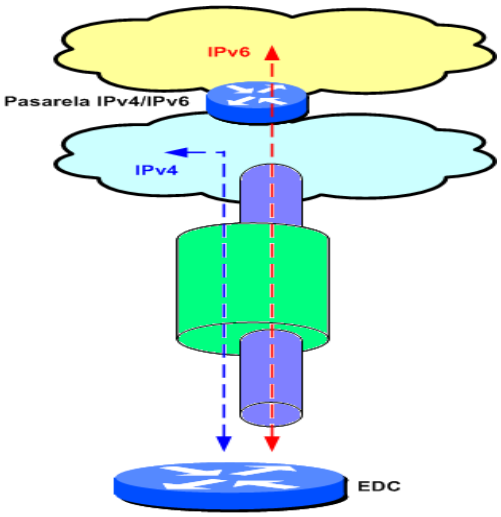


Figura 6.4.24 Esquema de conectividad de IPv4 con IPv6.Elaboración propia.

6.4.7.4 Servicio Acceso a Intranet

6.4.7.4.1 Descripción del servicio

El Servicio Acceso a Intranet tiene como objetivo trasladar las mismas condiciones y recursos de comunicaciones con los que cuenta un trabajador en su empresa, a su ubicación remota. El Servicio permite disponer de **acceso remoto a la Intranet de la Empresa**, acercando **de forma segura las herramientas de trabajo diario** (aplicaciones e información corporativa) a sus empleados en cualquier lugar donde se encuentren. La comunicación entre los Usuarios (empleados) hacia la empresa se realiza bien de forma **privada** desde las diferentes redes de acceso disponibles: RTB, RDSI, GSM y XDSL sobre la red de Telefónica de España **mediante túneles L2TP (modalidad PRIVADA)** o bien sobre **Internet** mediante el uso de **túneles IPSec (modalidad PÚBLICA).**

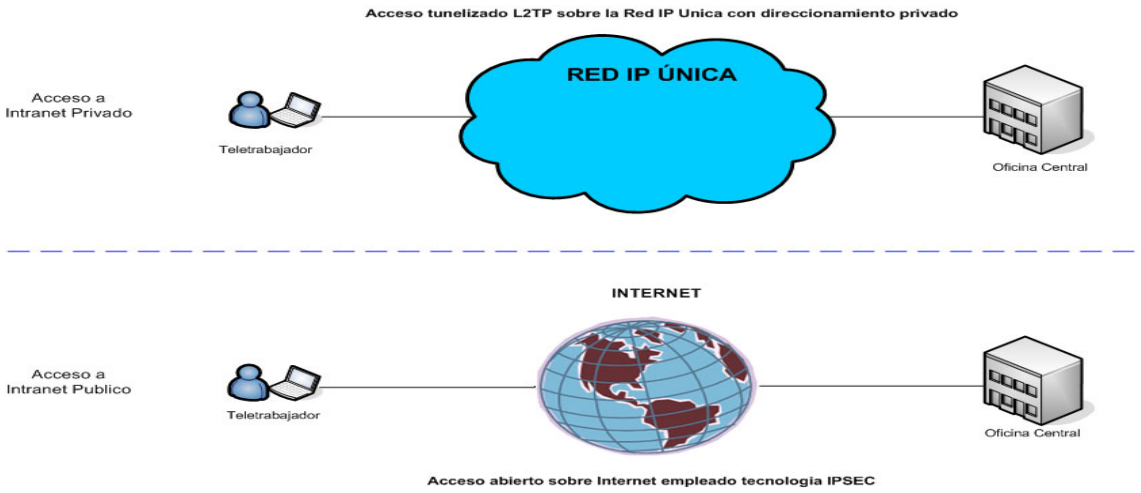


Figura 6.4.25 Esquema general de acceso a Intranet en modalidad pública y privada.Elaboración propia.

Los usuarios, desde sus ubicaciones remotas, acceden al servicio mediante conexiones conmutadas (RTB, RDSI o GSM) o por ADSL. Mediante un **nombre de usuario del tipo (usuario@empresa.es) accederán a la corporación para ser autenticados**. Una vez el acceso ha sido autorizado, tendrán acceso a la Intranet de la empresa. La corporación tendrá una **conexión permanente a la Red IP Única**. A través de esta conexión recibirá todo el tráfico de datos procedente de los usuarios remotos. Para saber a modo resumen las caracteristicas y las dos modalidades de servicio consultar el documento **memoria_anex.pdf apartado ANEXO31.**

6.4.7.4.2 Modalidad Privada

El usuario remoto podrá acceder a través de ADSL, o bien, desde un acceso conmutado, RTB, RDSI o GSM, a la Intranet de su corporación. La corporación estará conectada, **mediante un acceso permanente, a la Red IP Única**. Para el acceso a la corporación, los **usuarios remotos iniciarán una sesión PPP**. Esta sesión PPP se prolongará hasta la corporación **mediante el establecimiento de un túnel L2TP**. Este túnel se establece entre el servidor de acceso (LAC) y el servidor de túneles (LNS) de la corporación. Al establecer la sesión PPP, el usuario remoto habrá introducido un nombre de usuario (en la forma: usuario@dominio) y una clave de acceso. Este nombre de usuario y esta clave son validados de acuerdo a uno de los **dos modelos de autenticación** contemplados en el servicio (**Modelo de Autenticación Delegada y Modelo de Autenticación en Red).**

Para saber las caracteristicas completas del modelo de autenticación delegada y en red consultar **el documento memoria_anex.pdf apartado ANEXO32.**

En este proceso es indispensable que el servidor de túneles de la corporación sea visible en la Red IP Única de forma que se pueda establecer el túnel L2TP contra él. Por tanto, la corporación deberá disponer de una conexión permanente a la Red IP Única, a través de la cuál recibirá todo el tráfico procedente de los usuarios remotos. La siguiente figura muestra un esquema general con la arquitectura de la modalidad privada.

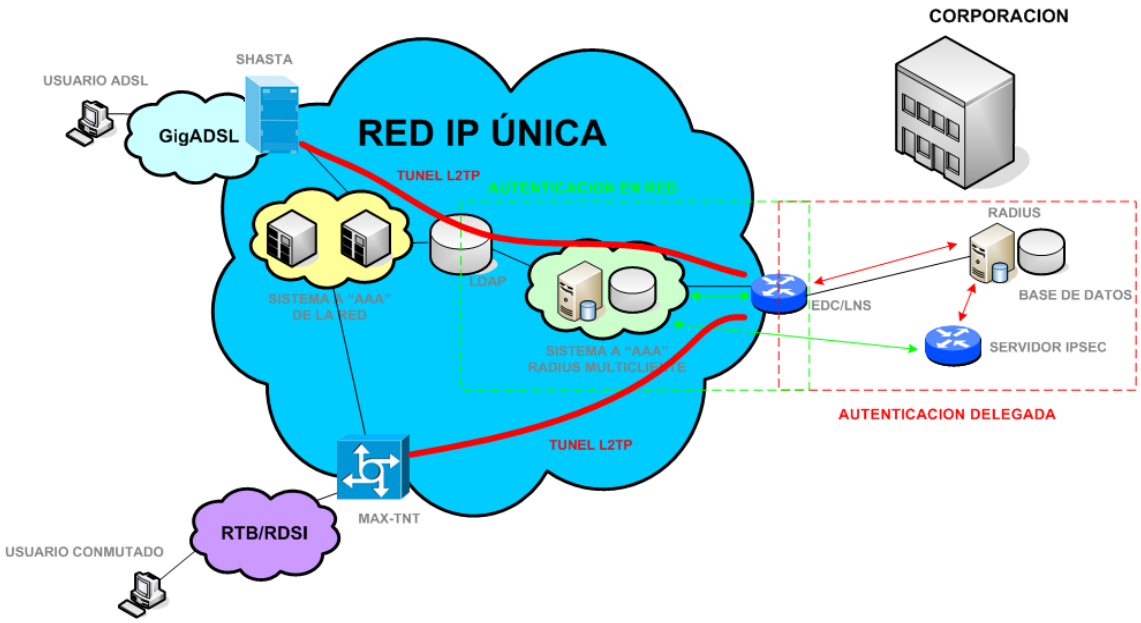


Figura 6.4.26 Arquitectura de red de la modalidad privada del acceso a Intranet.Elaboración propia.

6.4.7.4.3 Modalidad Pública

La modalidad pública del servicio **consiste en llevar el tráfico cifrado (IPSec) desde los usuarios remotos hasta la corporación teniendo como único requisito que el usuario tenga acceso a Internet.** También es requisito imprescindible que la corporación esté visible en Internet. **El tráfico de los usuarios remotos se transporta mediante túneles IPSec hasta la corporación.** Los túneles IPSec, a diferencia de los L2TP, arrancan desde el PC de los usuarios remotos. Una vez que el usuario remoto está conectado a Internet, establecerá desde su PC un túnel IPSec hasta un servidor de túneles que se encuentra en la corporación.

Cuando el túnel IPSec se establece, el tráfico original que genera el usuario remoto se cifra en su tránsito por la red pública y cuando llega a la Intranet del cliente es descifrado por el Servidor de túneles IPSec. De esta forma para el usuario remoto es como si fuera parte de la red privada de cliente y puede por tanto, acceder a las aplicaciones internas de forma segura.

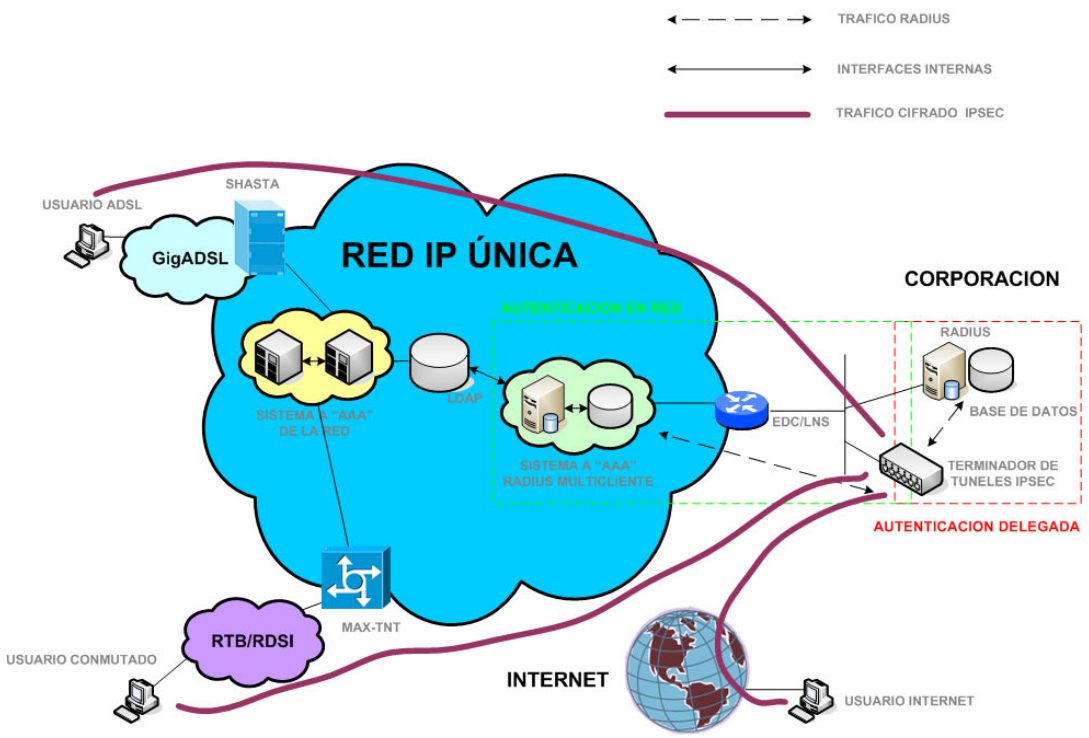


Figura 6.4.27 Arquitectura de red de la modalidad pública con IPSEC del acceso a Intranet. Elaboración propia.

6.4.7.5 Servicio IBERCOM IP

6.4.7.5.1 Descripción del servicio

En el modelo de **arquitectura de Telefonía IP Corporativa**, todos los fabricantes tienden a aproximarse a un mismo **modelo basado en un equipamiento compuesto** por:

- **Gestor de llamadas** (Call Server o Media Server) que se encarga del control de los teléfonos, gateways y llamadas mediante protocolos específicos.
- **Gateways** que permiten la interconexión con el mundo analógico tradicional.
- **Teléfonos IP**.

Por tanto, el servicio Ibercom IP de Telefónica los que ofrece es **un servicio gestionado de Telefonía IP Corporativa** basado en una **infraestructura específica para cada cliente** que principalmente **contendrá los elementos anteriormente indicados**.

Ibercom IP usa y **convive** perfectamente con los **servicios de transporte de datos mediante RPVs convergentes**, es decir, una red que soporta tanto el transporte de aplicaciones tradicionales como las nuevas aplicaciones de Telefonía IP de las empresas con la calidad requerida y que **permite integrar dentro de una misma plataforma tecnológica las comunicaciones de voz, datos e imágenes**, con **acceso a las distintas redes existentes**, tanto públicas **(RTB/RDSI, NGN y Móvil) como privadas (red IP de cliente).**

La contratación por parte de un cliente del servicio Ibercom IP, lleva asiada **siempre la existencia de un servicio de RPVs de datos convergente**, que puede ser: VPN IP o MacroLAN ya que aunque inicialmente estos servicios se diseñaron para transportar comunicaciones de datos, con el auge de las aplicaciones de VoIP, se pretende utilizar dichas redes con este tipo de aplicaciones.

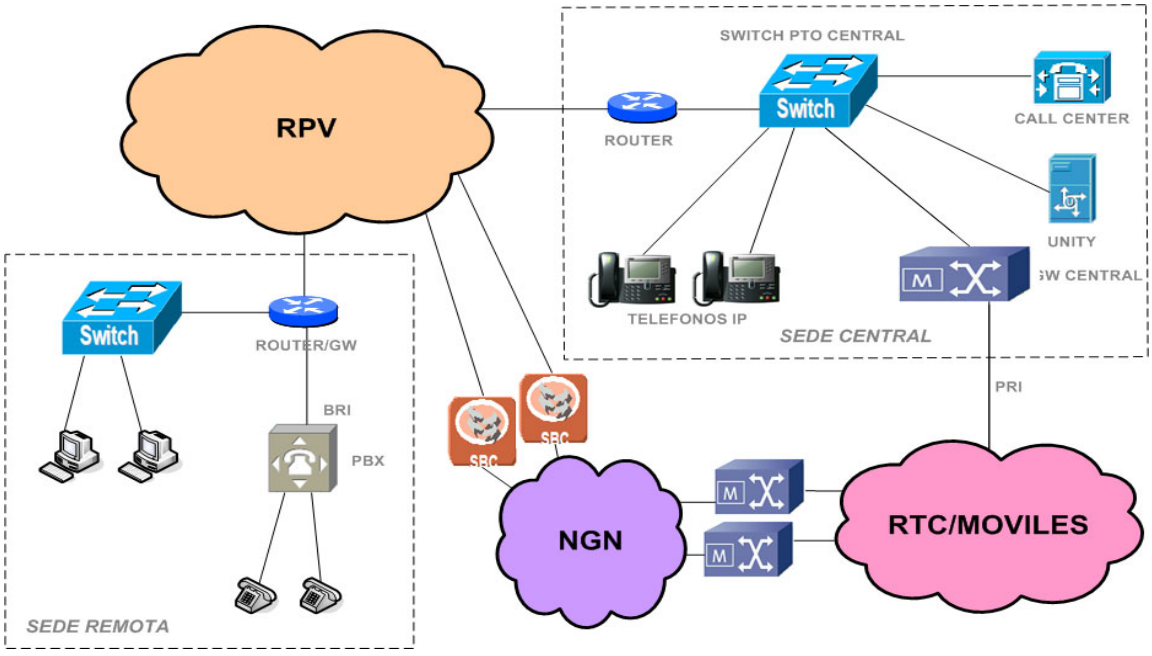


Figura 6.4.28 Arquitectura general del servicio Ibercom IP.Elaboración propia.

El servicio Ibercom IP propone la migración de la clásica telefonía tradicional a una infraestructura basada en VoIP **cuyos beneficios** se basa en:

- **Evolución tecnológica de los proveedores de servicios y equipamiento**: Los suministradores de equipamiento ya no fabrican nada que no sea IP porque les resulta más fácil y más barato que las tecnologías tradicionales. Esto va a llevar a situaciones en X años en los que los repuestos y las nuevas adquisiciones de equipamiento (hardware, placas, terminales,...) basado en tecnologías tradicionales no se suministren o sean muy caros con respecto a las tecnologías IP. Además los operadores como Telefónica, evolucionan sus redes a IP en todos los entornos. Esto es muy acusado en la parte "fija" pero los móviles es el siguiente paso. A efectos del cliente se traduce en que los operadores invertirán en accesos en IP (por ej. el ADSL ya evoluciona el ATM a IP).
- **Universalización de los servicios finales de usuario**: La VoIP no "restringe" el número de funcionalidades básicas disponibles por tecnología tradicional (desvíos, transferencias, multiconferencias, retrollamada, rellamada,...). Tampoco aporta ninguna funcionalidad básica asociada a la voz tradicional. La VoIP universaliza los servicios a los que puede acceder el cliente a todas las extensiones e incluso permite disponer de esos servicios entre extensiones que se encuentran en ubicaciones diferentes. En entornos tradicionales los servicios dependen de la centralita que esté instalada en la dependencia donde está el teléfono y en general no "circulan" los servicios entre sedes con centralitas diferentes.
- **Integración de la voz con aplicaciones de PC y cliente**: En este entorno claramente la VoIP es imprescindible ya que con tecnología tradicional no es posible (no todas las cosas son directamente aplicables, algunas precisan una labor de integración). Entre las posibles aplicaciones se pueden destacar:
    - **Integración de correo y buzón de voz**:
        - Recibir los mensajes vocales de voz en la aplicación de correo.
        - Escuchar los correos (text to speech) desde el teléfono.
        - Gestionar, borrar,... los mensajes desde cualquier entorno (correo, buzón,...).
    - **Gestor de llamadas:** Acceso desde una página web a un entorno personal en el que puedes programar perfiles de desvíos o transferencias de llamadas en función de diferentes parámetros (horario, llamante, estado,...).

- **Comunicador**: Es un software de PC asociado a un terminal de teléfono IP que permite ver el estado de presencia de los usuarios, llamar, desviar, transferir,...
- **Mensajería instantánea (chat).**
- **Envió/recepción de SMS/MMS** a través del PC.
- **Directorio corporativo:** Integración con los directorios corporativos de manera que exista un único repositorio de la empresa que contenga toda la información de directorio (nombre, correo, teléfonos,...) accesible desde cualquier terminal.
- **Click-to-call:** Para poder llamar clicando en el PC sobre el nombre del directorio sin necesidad de conocer el número y el identificador.
- **Barras de herramientas en Ofimatica de ToIP**: para poder llamar desde cualquier aplicación ofimatica (más normal en el correo).

- **Movilidad y desplazamientos:** El usuario de VoIP viaja con la persona y, siempre que haya un teléfono IP y acceso a la red corporativa de cliente, el usuario se puede "logar" y disponer de los mismos servicios de telefonía.
- **Videocomunicaciones:** Realización de videollamadas entre terminales y PCs. Multivideoconferencia corporativa para todos los usuarios (no sólo para las salas). Evolución a Videollamadas corporativas fijo-móvil.
- **Mayor disponiblidad de información de uso:** Al tener un único (o pocos en número) repositorios de información o servidores es más fácil la realización y personalización de los informes de uso. De otro modo, con elementos distribuidos y tecnología tradicional, es necesario extraer la información de todas y cada una de las centralitas.

Evolucionar la telefonía tradicional a VoIP además de los beneficios anteriormente indicados, supone que **afectara a una serie de costes**:

- **Costes de cableado de edificios:** Con telefonía tradicional el cableado de los edificios debía contemplar una red para datos (ethernet) para los PCs, impresoras,... y otra específica de voz con tomas analógicas y digitales. Con la VoIP sólo es necesario un cableado Ethernet.

- **Costes de mantenimiento, electricidad y equipamiento:** Tanto si ese mantenimiento se lo realiza el propio cliente como si los hace el operador, el hecho de tener una centralita en cada una de las dependencias implica disponer de un espacio, una alimentación... y un mantenimiento .Se reduce con la disponibilidad de soluciones centralizadas en las que existe un número reducido de Call Managers/Servers (que incluso pueden estar en dependencias del operador) que dan servicio a todas las dependencias, con teléfonos remotos.
- **Costes asociados a movimientos, cambios, altas/bajas:** La VoIP permite disponer de "ubicuidad" ya que el usuario NO va asociado al terminal, con lo que cualquier cambio o modificación es mucho menos traumática.
- **Costes de administración de usuarios:** En un escenario con tecnología tradicional, el cliente se ve obligado a "tocar" en todas y cada una de las centralitas para que sean conscientes de dichas modificaciones. En el caso de VoIP lo puedes hacer desde una web directamente de una vez.
- **Costes de tráficos y accesos:**
    - Tráfico interno: En general pasan a ser 0 ya que se cursan por la red de datos.
    - Tráfico fijo-móvil: Permite concentrar el tráfico con destino móvil en el punto de interconexión con el operador móvil.
    - Accesos de voz: El tráfico interno no sale a la red pública por lo que precisa menos accesos.
    - Accesos de datos: Es necesario ampliar la capacidad del servicio de datos para cursar la voz.

6.4.7.5.2 Requisito de Adaptación de las RPVs a convergentes

Como he explicado anteriormente el servicio Ibercom IP se apoya en los servicios VPN-IP y Macrolan para el transporte de la voz junto con los datos. El **transporte de la voz** implica que se deben cumplir una serie de **requerimientos por parte de las RPV** para que la voz no se vea afectada, eso implica una adaptación de las RPVs tradicionales.

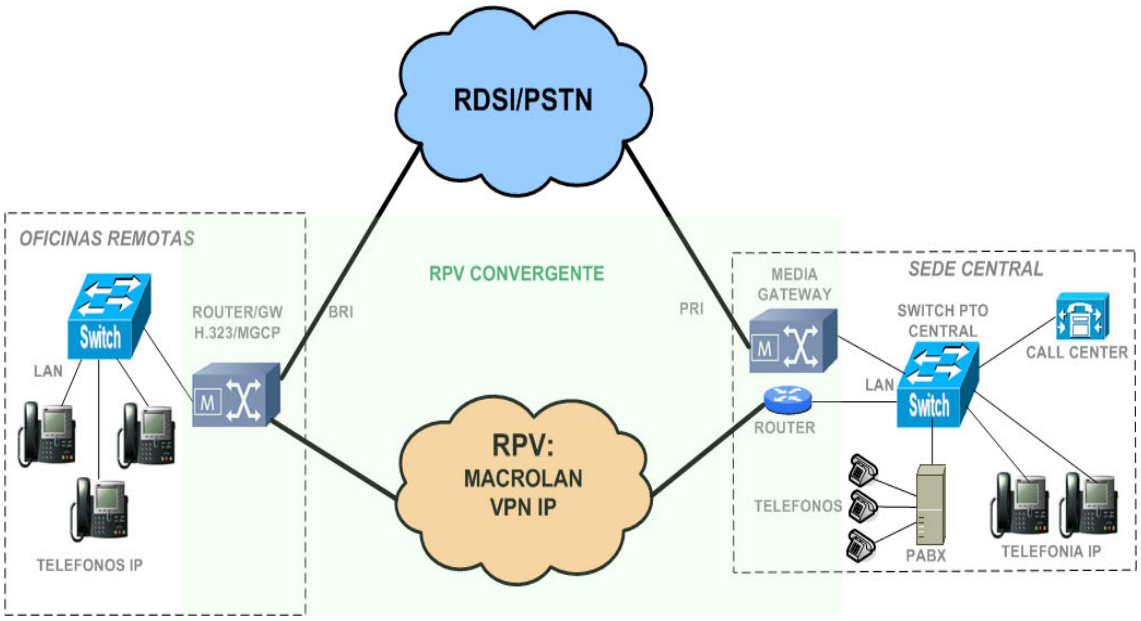


Figura 6.4.29 Arquitectura general de una RPV convergente.Elaboración propia.

En un primer análisis, la **convergencia de las redes de telefonía y de las redes de datos** se puede percibir a distintos niveles de integración.

1) Un primer nivel se produce cuando se **utilizan las líneas de comunicaciones de las redes de datos para realizar el transporte de señales de telefonía**, paquetizada sobre protocolo IP, lo cual va a exigir la aplicación de herramientas de QoS en los equipos de comunicaciones que forman la red. Para conocer con detalle los requisitos en materia de lantecia, jitter, perdida de paquetes…consultar el documento **memoria_anex.pdf apartado ANEXO33.**

2) Un segundo nivel de integración aparece cuando los terminales Teléfonos IP se despliegan sobre las redes de área local de las oficinas y plantea **nuevos requerimientos en la LAN** (separación de tráfico en distintas VLANs, seguridad, etc.). Los requerimientos LAN en los switches se puede consultar en el documento **memoria_anex.pdf apartado ANEXO33.**

3) El nivel de integración superior se tendrá cuando **determinadas funciones de la aplicación de Telefonía pueden ser proporcionadas por el mismo equipo terminal de las redes de datos EDC**, como son las funcionalidades de Gateway de Telefonía y de centralita local para situaciones de emergencia.

6.4.7.5.3 Elementos del servicio Ibercom IP

Una vez explicados los requisitos que han de cumplir las RPVs de la red IP Única y en la parte LAN para que el servicio Ibercom IP se preste con la máxima calidad y garantía, voy a indicar los elementos mínimos y sus funciones que componen el servicio.

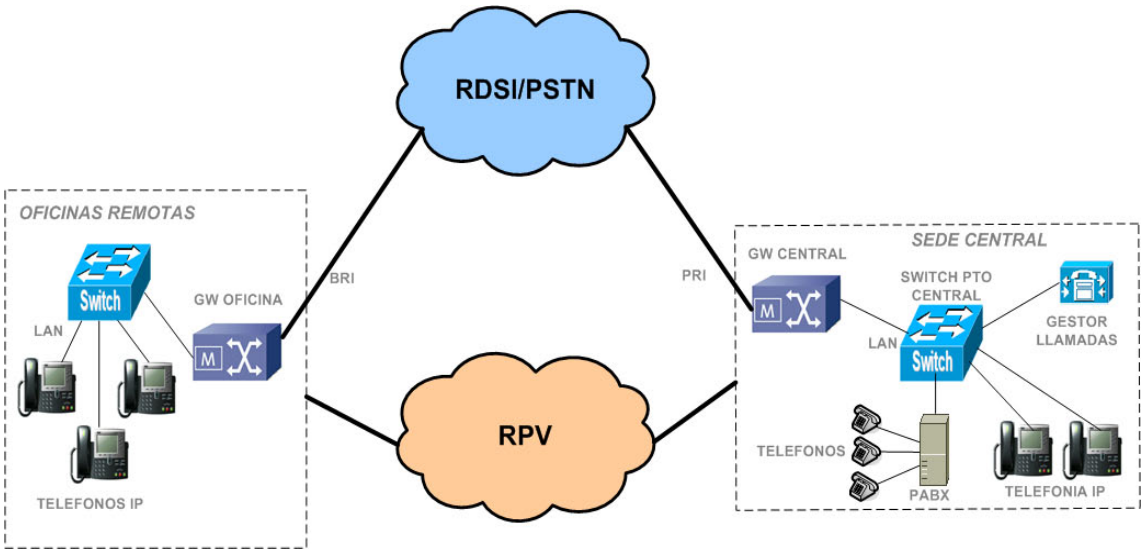


Figura 6.4.30 Elementos que conforman el servicio Ibercom IP.Elaboración propia.

- **Gestor de llamadas**: La principal función de este elemento de la solución es la de gestionar de manera centralizada la **conmutación de llamadas** de telefonía y multimedia. Proporciona la inteligencia centralizada a través del **directorio de usuarios** y la **gestión de recursos de la red** (Gateways y Teléfonos) y resuelve la **señalización** entre todos los elementos.
- **Gateway central (Trunking-gateway):** Es el elemento de la solución que proporciona la **interconexión** entre **el entorno de telefonía IP y el entorno de telefonía tradicional**, bien con las centralitas tradicionales en domicilio de cliente (PBX) como con la red pública (RTC). Adicionalmente, proporciona recursos de Transcodificación y Multiconferencia centralizados para determinados servicios telefónicos complejos.
- **Gateway de oficina:** Es el elemento de la solución que proporciona para una oficina remota la funcionalidad de **GW de telefonía** para **la interconexión local entre la telefonía IP y la red pública (RTC)**. Como router tiene la función de soportar el enrutamiento de tráfico de datos y de voz hacia el entorno central. En situaciones de aislamiento realiza además **funciones de centralita local** de

emergencia permitiendo la comunicaciones locales entre Teléfonos IP y **llamadas externas.**

- **Teléfonos IP:** Existen varios tipos de terminales telefónicos IP e incluso tienen cabida en la solución teléfonos convencionales conectados a través de adaptadores ATA.

6.4.7.5.4 Plan de numeración y Enrutamiento de llamadas de ToIP

Para la configuración de los Gateways Central y de Oficinas y por lo tanto para la RPV proporcione las funcionalidades necesarias a la **solución de Telefonía IP son requisitos necesarios conocer**:

- El **Plan de Numeración** tanto de las Oficinas como de los accesos RDSI locales.
- Los **planes de enrutamiento** de llamadas en Break-in (Llamadas entrantes desde la RTB) y en Break-Out (Llamadas Salientes a la RTB), locales o completas.

6.4.7.5.4.1 Plan de Numeración

Se debe de tener un **plan de numeración en el que no exista solapamiento de extensiones**.

6.4.7.5.4.2 Plan de Enrutamiento

Todas las llamadas entre los teléfonos corporativos se efectúan, **siempre que sea posible, a través de la red de datos corporativa RPV: Macrolan o VPN IP**. En esta RPV se ha de provisionar ancho de banda específico para el tráfico de voz (caudal multimedia). En funcion del tipo de llamadas que se realice por IP o externas existen diferentes modos de catalogar las llamadas. Para saber cada uno de los modos, consultar el documento memoria_anex.pdf **apartado ANEXO34.**

6.4.7.5.5 Escenarios del Servicio

Para proporcionar unos niveles adecuados de disponibilidad del servicio de Telefonía se disponen de diversas soluciones técnicas y de arquitectura que pueden estudiarse desde distintos ámbitos.

1) **Desde el ámbito de la RPV soporte** de la solución de Telefonía IP. En los Servicios de RPV MacroLan, VPN IP se proporcionan diversos escenarios de redundancia, con doble línea de acceso (principal y secundaría), e incluso escenarios de redundancia de equipos.
2) **Desde el ámbito de los sistemas de Telefonía** y sus elementos de servicio, las soluciones de Telefonía IP pueden proporcionar **redundancia de los Gestores de llamadas**, que atienden la señalización del resto de dispositivos de la solución. Estos elementos pueden a su vez situarse en diferentes Sedes Centrales agregando una **disponibilidad geográfica** a dichos elementos.

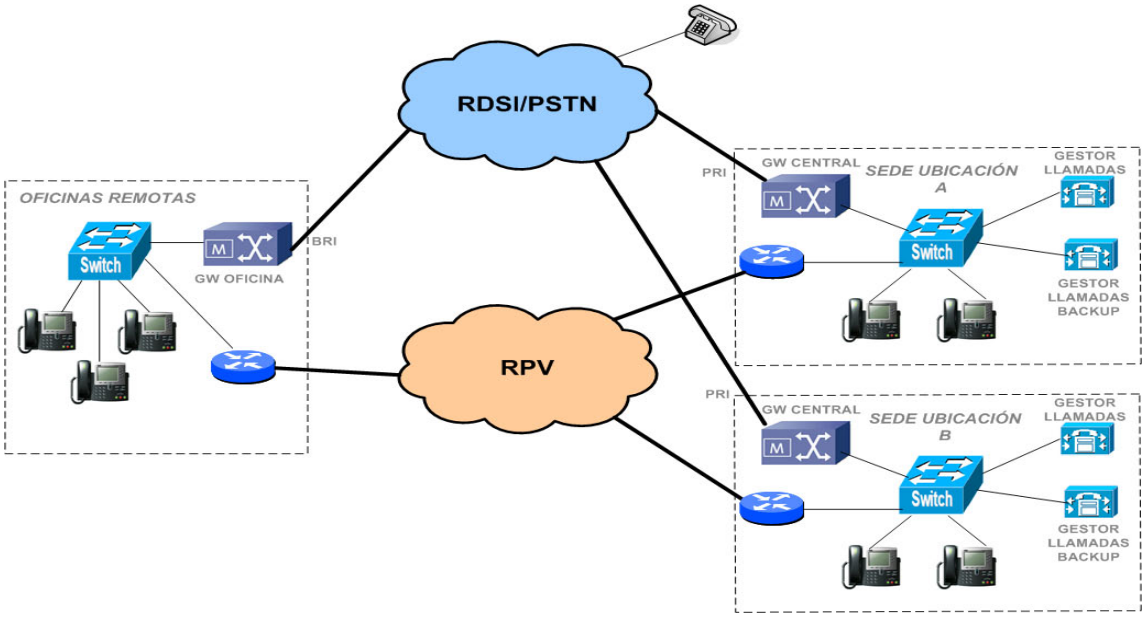


Figura 6.4.31 Redundancia de los gestores de llamadas por duplicidad y geográficamente.Elaboración propia.

3) **Desde el ámbito de los Gateways**, es de destacar la función **de Supervivencia de oficina** remota en el ámbito de las aplicaciones de Telefonía. Los Gateways incorporan dicha funcionalidad adicional de conmutación y gestión de llamadas entrantes y salientes en local, lo que proporciona un nivel de disponibilidad adicional a las soluciones de telefonía IP para los casos de aislamiento de la oficina remota de la red de datos, y permitiendo, con alguna restricción en las facilidades de llamada, las comunicaciones On-net y Off-net. Los **Teléfonos IP se registran con el GW, y las llamadas se cursan a través de la conexión RTB/RDSI local del GW**.

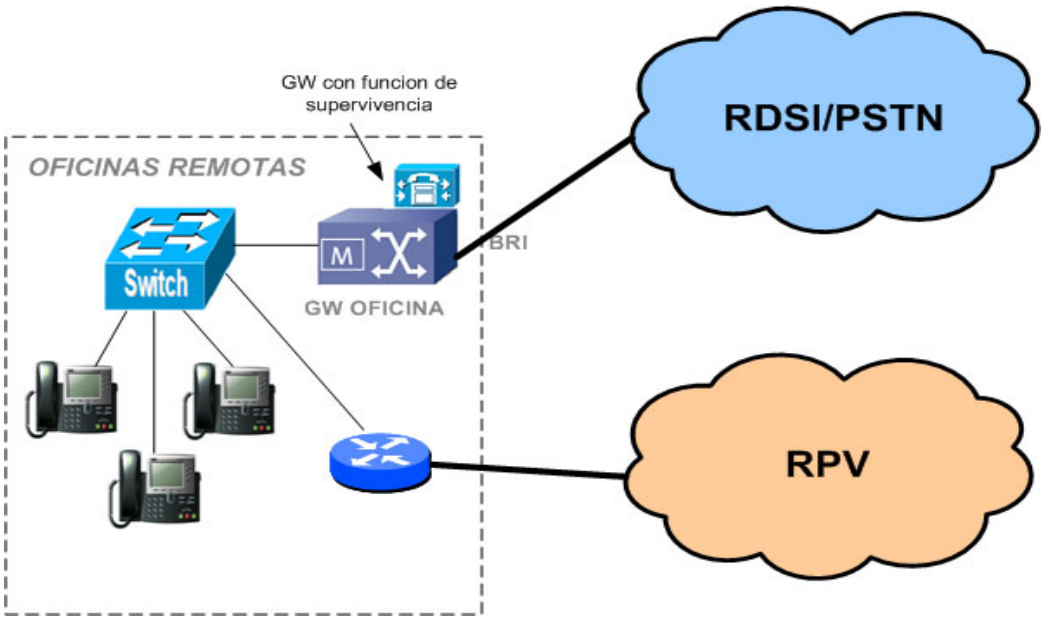


Figura 6.4.32 Gateway con función de supervivencia.Elaboración propia.

6.4.7.5.6 Servicios de Valor Añadido

El servicio Ibercom IP permite la contratación adicional de funcionalidades y servicios que permita satisfacer la necesidad del cliente. Dependiendo de la centralita instalada, se facilita contratar unos servicios u otros, pero a grandes rangos se permitiría en cualquier tecnología entre otros los siguientes servicios:

- **Aplicaciones de Administración y Gestión.**
- Aplicaciones de control de consumo **(tarificadores).**
- **Buzones de llamadas**.
- **Mensajerías:**
  - Mensajerías básicas y unificadas.
  - Integradas o externas.
- Herramientas para entornos de **Centros de Atención de Llamadas (Call Center)** como ACD, CTI,CRM…
- **Aplicaciones de telefonía sobre PC** como son los Softphone.
- Sistemas inalámbricos DECT/GAP.
- **Operadoras sobre PC.**
- **Videollamadas y multiconferencia sobre IP.**
- Servicios de Presencia.

6.4.7.5.7 Conexión con la red NGN

El servicio Ibercom IP permite tener una **conexión con la red NGN mediante de Accesos Primarios Virtuales**, que ofrece un interfaz de acceso que simulará la capacidad de comunicación de un Acceso Primario (30 comunicaciones simultáneas) mediante las capacidades de NGN y soportado en transporte con tecnología IP. **Dichas interfaces de conexión** se ofrece a estos clientes a través de una interconexión entre la Red IP y la Red NGN, **para los servicios de RPV: MacroLan, VPN IP** .Las RPVs están capacitados para dotar esta interfaz de conexión con la Red NGN a través de los SBCs.

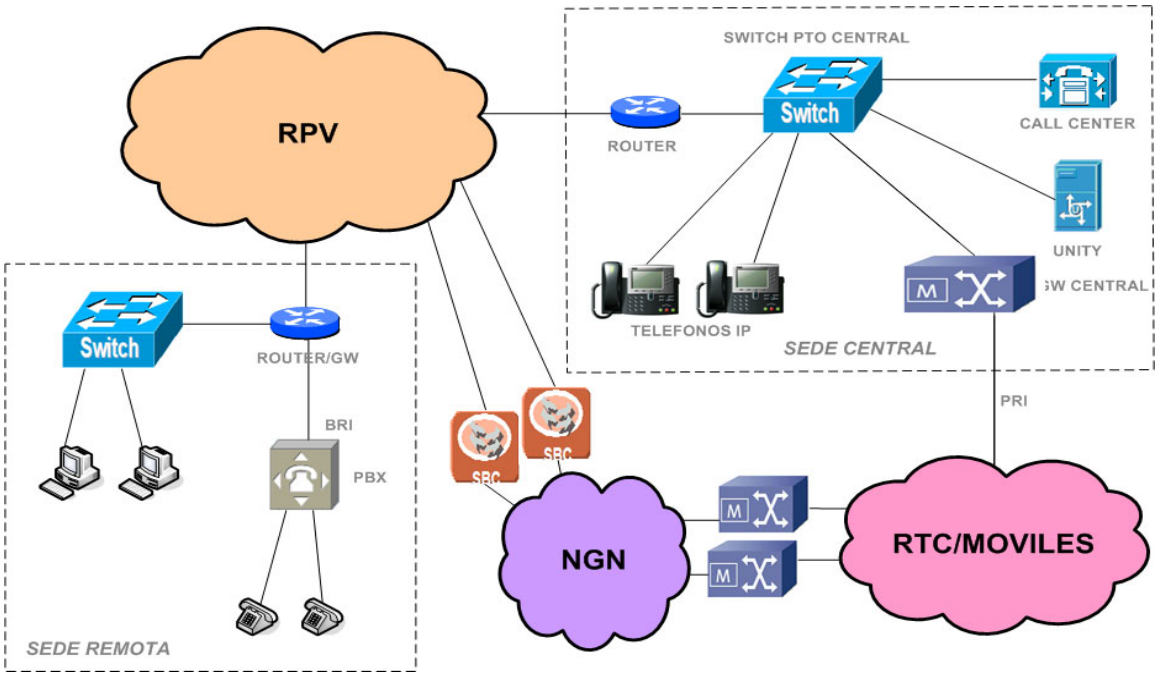


Figura 6.4.33 Interconexion del servicio Ibercom IP con la red NGN.Elaboración propia.

6.4.7.6 Servicio NETLAN

6.4.7.6.1 Descripción del servicio

El Servicio NETLAN se define como un **servicio de Redes Privadas Virtuales orientado a la PYMES, Negocios y Profesionales.** Así, como los servicios VPN-IP y MACROLAN están pensados para Grandes Clientes y Empresas, el servicio Netlan lo es para pequeños clientes. Las características de los servicios serian las siguientes:

- Para gran empresa: VPN-IP y MACROLAN
  - Seguridad y privacidad.
  - Diseño a medida de las necesidades del cliente.
  - Instalación y configuración de los edcs manuales.
  - Gestión manual.
- Para PYMES: Netlan
  - Seguridad y privacidad.
  - Diseño de catalogo.
  - Instalación y configuración de los edcs semiautomáticas.
  - Gestión automática.
  - Bajo coste.

Los elementos que componen el servicio Netlan son:

- Conectividades entre distintas dependencias.
- Sedes.
- Accesos remotos.
- Gestión central.
- Otros servicios.

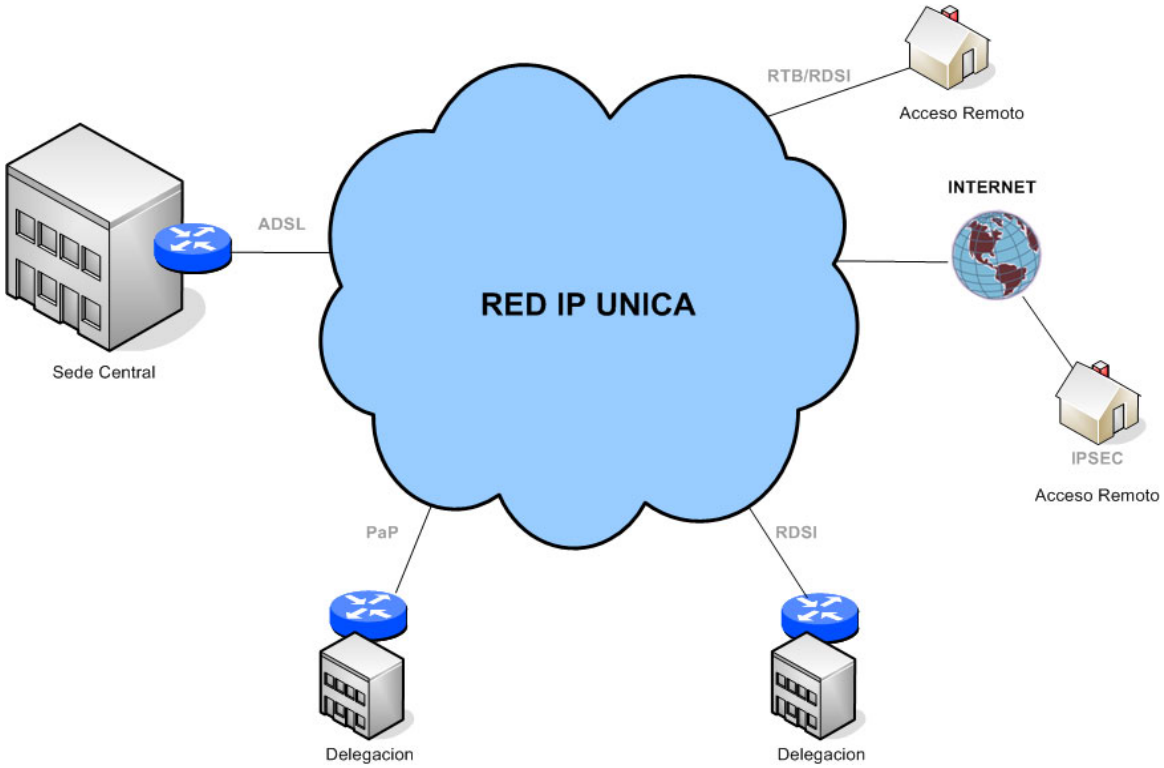


Figura 6.4.34 Esquema general del servicio Netlan.Elaboración propia.

Respecto a las **topologías de red** que permite el servicio Netlan se contemplan:

- **Estrella.**
- **Malla.**
- **Mixta.**

Para conocer las modalidades de contratación del servicio Netlan, asi como los diferentes tipos de acceso y sus facilidades adicionales, **consultar el documento memoria_anex.pdf apartado ANEXO35.**

6.5 RED NGN

En el año **2003 Telefónica definió la arquitectura de Red de Nueva Generación (NGN) para la evolución de la Red Telefónica Básica** con la estrategia de evolución a una Red IP universal "Todo IP", así cómo para el soporte de nuevos servicios multimedia. En la especificación de esta **arquitectura se seleccionó la tecnología IMS (IP Multimedia Subsytem) cómo núcleo de control.**

6.5.1 Requisitos arquitectura NGN

En forma general la arquitectura de una Red de Nueva Generación **deberá cumplir con los siguientes principios o requerimientos** que se relacionan a continuación:

- Funcionalmente se basará en **una arquitectura de red horizontal** con una división de los **planos de Transporte, Control y Aplicación**.

- El **plano de transporte** se basará en **tecnología de conmutación de paquetes IP/MPLS** y accesos banda ancha fijos y móviles.

- Estará **constituida por Entidades funcionales bien definidas**, así mismo, la comunicación entre estas entidades funcionales será vía interfaces abiertas y protocolos estandarizados.

- Debera soportar los actuales servicios telefónicos y servicios básicos dentro de las capacidades globales de la red.

- Deberá **garantizar el interfuncionamiento con las actuales redes** existentes.

- Dispondrá de **separación dentro de las funciones de control**, en control de recursos en la capa de acceso/transporte, control de llamada/sesión y control de aplicación/servicio.

- La **definición y provisión de servicios y acceso a los servicios será independiente de la tecnología** de la Red, tanto en su plano de control, cómo en su tecnología de acceso sea esta última fija o móvil.

- **Soportará servicios de diferente naturaleza**, incluyendo servicios real time, streaming, non-real time y con capacidades multimedia (Voz, video, texto), combinados en una misma sesión.

- Dispondrá de capacidades para **ofrecer servicio de banda ancha con transparencia extremo a extremo** con calidad de servicio (QoS) garantizada.

- **Seguridad en el acceso**, en la disponibilidad de la Red, en la integridad de las comunicaciones, así cómo seguridad física y lógica dentro y entre las diferentes áreas, zonas y dominios IPs configurados para su prestación en la Red.

- **Movilidad generalizada**, acceso a los mismos servicios desde cualquier aplicación/dispositivo (movilidad entre dispositivos/aplicaciones), cualquier tecnología de acceso (movilidad entre diferentes redes de acceso fija o móvil), cualquier red de operador (movilidad entre redes de operador roaming o nomadismo).

6.5.2 Arquitectura NGN

La siguiente figura representa una visión esquemática de la separación entre plano de esta arquitectura.

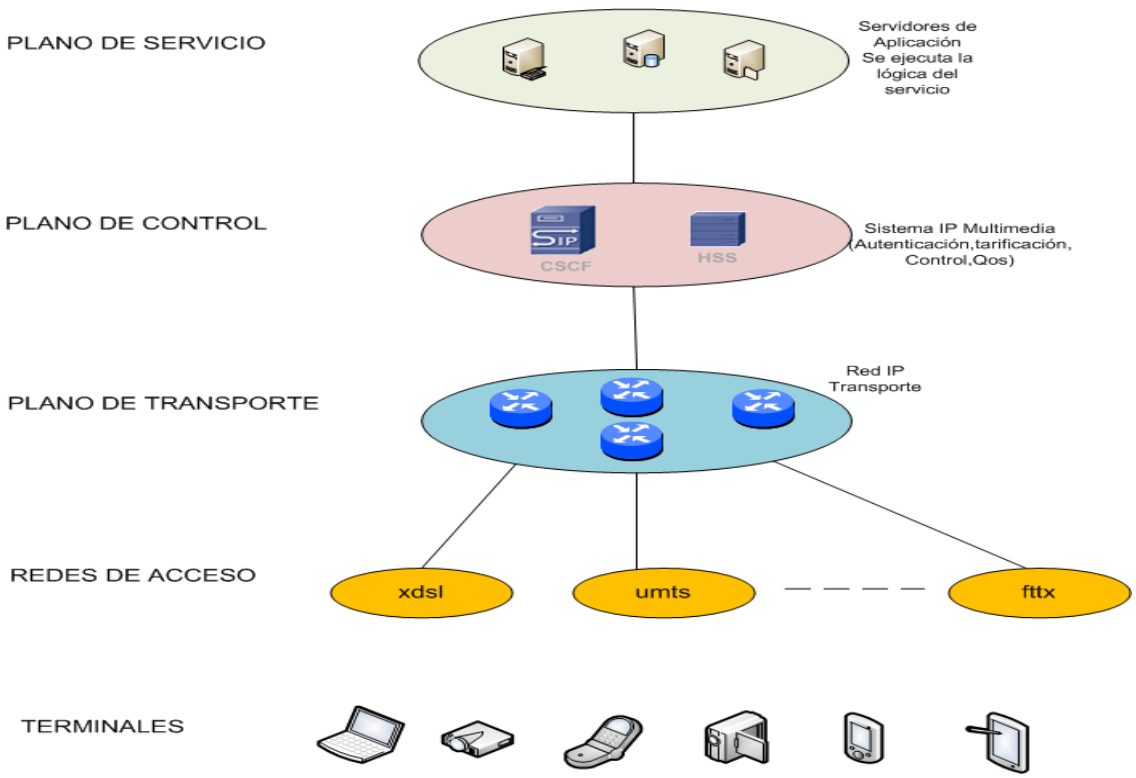


Figura 6.5.1 Capas que componen la arquitectura de la red NGN.Elaboración propia.

De forma abreviada, se enumeran a continuación los diferentes planos y sus funciones:

- **Redes de acceso banda ancha**: La red NGN soportará el acceso a sus servicios desde las diferentes redes de acceso banda ancha fija o móviles. Para garantizar la transparencia se implementan en la Red funciones de integración e interacción con las distintas redes de acceso para el control de recursos en la misma, así cómo para el intercambio de información que se adaptarán para su uso o presentación al resto de los planos y aplicaciones de forma transparente.
- **Plano de transporte IP/MPLS**: Se basa en una Red IP/MPLS común, cómo soporte de todas la comunicaciones, e independiente de las redes de acceso.
- **Plano de control IMS:** Realiza las funciones comunes para todos los servicios relativas a la autenticación de clientes, autorización para acceso y uso de la red (registro), autorización para acceso a los diferentes servicios, funciones de tarificación unificada en línea o fuera de línea por el uso de la red y/o los diferentes servicios, control de las sesiones de los usuarios y de la invocación de lógica de los servicios, control de asignación de recursos y calidad de servicio, etc.

- **Plano de Aplicación:** En este plano se ubican de forma simplificada los diferentes servidores de aplicación donde se ejecuta la lógica de los servicios finales de cliente, o de forma más genérica los distintos elementos que a su vez componen la arquitectura funcional de los entornos de creación de servicio, para el desarrollo, ejecución y prestación de servicios finales.
- **Terminales y/o Aplicaciones de Cliente**: Forman un componente esencial dentro de la arquitectura de red de nueva generación o con mayor precisión dentro de la Arquitectura de Servicios de Nueva Generación. A través de ellos los clientes acceden a los servicios.

Cómo se puede ver en la anterior figura, Telefónica ha definido una Arquitectura de Red de Nueva Generación basada en su **plano de control en el subsistema IP Multimedia Subsystem (IMS)**.

6.5.3 Elementos que componen la red NGN

A continuación se indican los elementos que forman parte del Núcleo de la Red IMS de TdE. En la siguiente figura se muestra una arquitectura general de la solución IMS/NGN en Telefónica España, donde se pueden identificar los elementos.

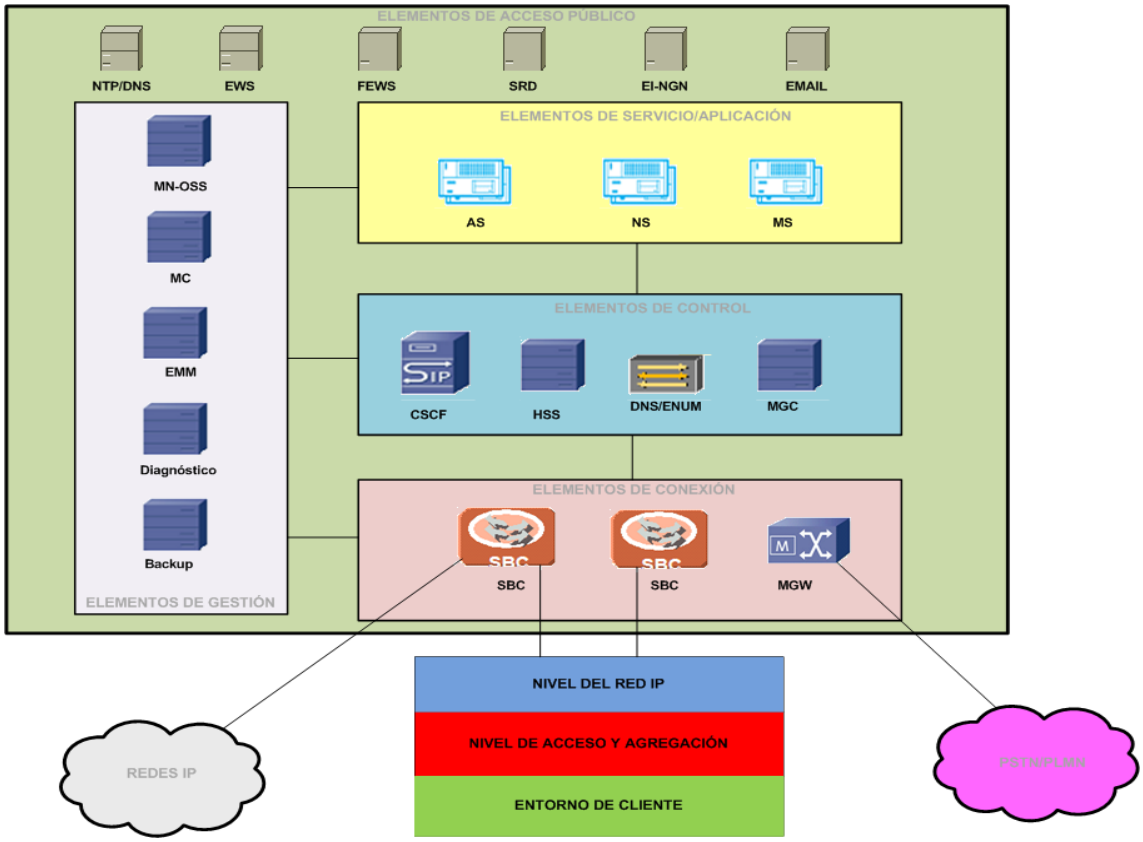


Figura 6.5.2 Arquitectura general de la solución IMS-NGN. Elaboración propia.

6.5.3.1 Elementos de control

Son denominados así las máquinas que han de **comunicarse entre sí mediante flujos de señalización o control que permiten establecer comunicaciones**, servicios o facilidades de la plataforma.

6.5.3.1.1 Call Session Control Function (CSCF)

La entidad funcional clave en una arquitectura IMS es el nodo CSCF (Call State Control Function), que básicamente **es un servidor SIP con funciones de Proxy**. El CSCF ejecuta tres "roles" diferentes en la operativa de IMS: Proxy CSCF (P-CSCF), Serving CSCF (S-CSCF) e Interrogating CSCF (I-CSCF):

- **P-CSCF:** El Proxy CSCF (P-CSCF) es el punto de entrada a una Red IMS. Recibe directamente la señalización IMS desde los terminales. Implementa las funciones de protección de la señalización (seguridad) y control de los recursos del Subsistema de Transporte. Además, ejecuta las funciones comunes a los demás CSCF: procesado y enrutado de señalización, consulta de perfil de usuario en el HSS y tarificación.
- **S-CSCF:** A cada usuario registrado en una Red IMS se le asigna un Serving CSCF (S-CSCF), el cual se encarga de enrutar las sesiones destinadas o iniciadas por el usuario. También realiza el registro y autenticación del abonado IMS y la provisión de los Servicios IMS. Asimismo genera los correspondientes registros de tarificación.
- **I-CSCF:** es el nodo intermedio que da soporte a la operación IMS. El I-CSCF ayuda a otros nodos a determinar el siguiente salto de los mensajes SIP y a establecer un camino para la señalización. Durante el registro, el P-CSCF se ayuda del I-CSCF para determinar el S-CSCF que ha de servir a cada usuario.

6.5.3.1.2 Home Subscriber Server (HSS)

HSS **es la BBDD maestra de la solución IMS que almacena y gestiona el perfil del Servicio IMS** del abonado, almacena las claves de seguridad y genera vectores de autenticación, registra el estado de los abonados y almacena el nodo S-CSCF con el que el abonado se ha registrado. El HSS actúa como BBDD de perfiles, localización, autenticación, autorización y gestor de registros. Proporciona las siguientes funcionalidades:

- **Generación de la información de seguridad** del Cliente. Genera los datos de autenticación e integridad con el propósito de proteger la red contra el uso no autorizado.
- **Soporte de la seguridad del Cliente**. Soporta la autenticación del acceso del Cliente hacia los Servicios Multimedia.
- **Identificación.** Almacena las relaciones apropiadas entre la identidad privada que identifica al Cliente y la identidad pública utilizada para el establecimiento de la llamada, esto es, SIP URL, E.164, …
- **Autorización del acceso.** Decide si el Cliente tiene los permisos necesarios para acceder a los Servicios Multimedia.
- **Gestión de la movilidad.** Ejecuta los procedimientos de gestión de la movilidad tal y como han sido descritos en las especificaciones del 3GPP.
- **Soporte de la información de los Servicios.** Proporciona el soporte para el almacenamiento de la información de disparo de Servicios, identidades del Servidor de Aplicaciones y claves de Servicio.

6.5.3.1.3 DNS/ENUM

Elemento que integra las entidades funcionales de ENUM y DNS.

Funcionalidad ENUM

Las Redes NGN se basan en el concepto de Red Única, la cual tiene que satisfacer los requisitos impuestos por cada una de las Redes existentes hasta ahora de manera diferenciada (red telefónica básica, redes móviles, redes IP,…). En este escenario surgen diferentes propuestas que actúan de catalizadores, como el protocolo **ENUM (nuevo protocolo de "numeración IP")**, que permite la **comunicación entre teléfonos convencionales y teléfonos IP**, siendo un claro facilitador del proceso de convergencia de redes.Para saber con detalle en que consiste el protocolo ENUM, consultar el documento memoria_anex.pdf apartado **ANEXO36.**

Funcionalidad DNS

Sistema de Nombres de Dominio (Domain Name Server). **Es un sistema que permite asignar nombres a equipos/nodos y servicios que se organiza en una jerarquía de**

dominios. Las Redes IP usan DNS para buscar equipos y servicios mediante nombres descriptivos. Puesto que IMS está basado en un mundo "Todo IP", la utilización de la funcionalidad DNS será precisamente esta, **asignar nombres a nodos y servicios concretos dentro de la arquitectura IMS**.

El elemento **DNS/ENUM es crítico**, puesto que está involucrado en un número importante de comunicaciones. Actualmente el servidor DNS/ENUM presta las siguientes funcionalidades:

- **Servidor DNS para resoluciones de nombres de máquinas a direcciones IP**, ante la consulta de los diferentes elementos del Núcleo de la Red IMS (SBC, HSS, CSCF, MGC/MGW,…).
- **Servidor ENUM para la traslación de identidades Tel URI** (E.164) **a identidades SIP URI** (usuario@ dominio).

6.5.3.1.4 Media Gateway Controller (MGC)

Elemento que **permite la interoperatividad entre el Núcleo de la Red IMS y las redes tradicionales de conmutación de circuitos**. Este elemento junto a las pasarelas de voz (MGW) que controla (mediante protocolo H.248) son los componentes esenciales de la arquitectura en las fases iniciales de despliegue, al contemplar mayoritariamente escenarios de llamadas con origen o destino usuarios de la RTB (Red Telefónica Básica) ó PLMN (Núcleo de Circuitos Móviles).Como elemento intermedio entre redes, **el Media GateWay Controller gestiona la señalización SIP del lado IMS-NGN en su relación con una red cuyo control está basado en ISUP**.

6.5.3.2 Elementos de conexión

6.5.3.2.1 Session Border Controller (SBC)

El SBC, en configuración de cluster, aporta el control de las comunicaciones entre usuarios y entre éste y el elemento de control de la solución de ambos dominios. **Se comporta como un proxy SIP tanto para el tráfico de media** (audio, video, etc) **como de señalización, y se implementa en el borde de la red IP para ofrecer entre otras funcionalidades, seguridad, control de acceso y admisión, o resolver los problemas de NAT transversal.**

6.5.3.2.2 Media Gateway (MGW)

Es el elemento encargado del **manejo de los datos de media intercambiados entre IMS y redes de circuitos (RTB ó PLMN)**. A través de su mediación se permite **adaptar la codificación de la voz (IP <->TDM) mediante el uso de Procesadores Digitales de Señal (DSP)**, por lo tanto incide de forma notable en la percepción de la calidad del servicio.

6.5.3.3 Elementos de servicio/aplicación

6.5.3.3.1 Aplication Server (AS)

La labor principal de este elemento es **ejecutar las lógicas de los servicios contratados por el cliente** tanto para el mundo residencial como empresarial. A través de un **servidor web externo (EWS)**, los clientes son provisionados en el AS mediante asignación individual o en grupo.

6.5.3.3.2 Network Server (NS)

Este elemento **permite proporcionar los servicios soportados en la red**, para ello **controla todos los recursos de ésta para encaminar las llamadas hacia la RTC**, así **como el direccionamiento a utilizar para alcanzar a cualquier usuario conectado a la solución**.

6.5.3.3.3 Media Server (MS)

Implementa funciones tales como **el establecimiento de audioconferencia** hasta tres usuarios**, portal de voz** con grabación de mensajes personalizadas por usuario, **buzón de voz, detección de dígitos DTMF** en menú interactivo (IVR) o para la introducción de códigos asociados a servicios (Account Code y Authorication code), etc. El nodo MS implementa los codec G.711 y G.726, así **como los protocolos RTP, RTCP, SIP, SMTP, HTTP y SNMP incluyendo MIBs para "Performance Management".**

6.5.3.4 Elementos de acceso público

6.5.3.4.1 Servidor NTP/DNS

El NTP server es el encargado de **proporcionar el sincronismo de tiempos al terminal del cliente**. El terminal deberá tener configurado este servidor, y su referencia deberá ser la misma que para el resto de nodos de AS. En cuanto a la funcionalidad DNS, sustituirá a la resolución de direcciones que actualmente lleva a cabo los DNS de RIMA mediante el

protocolo de encaminamiento IS-IS. Para ello implementa la funcionalidad Views de acuerdo al **BIND v.9 (Berkeley Internet Name Domain).**

6.5.3.4.2 External Web Server (EWS)

Soporta **las tareas de administración por parte de los gestores de la plataforma** así como de los usuarios finales mediante protocolo HTTP/HTTPS, para la gestión y provisión de la plataforma. Esta aplicación en principio integrada en el Aplication Server y externalizada por motivo de seguridad.

6.5.3.4.3 Front End EWS (FEWS)

Sistema que **permite al acceso directo de los usuarios al portal web de la plataforma**. La funcionalidad básica consiste en redirigir al usuario a partir de su identificación (número de teléfono IP) y contraseña al EWS del dominio EMM donde esta registrado.

6.5.3.4.4 Service Repository and Directory (SRD)

Elemento sobre el que el Front End **realiza las consultas para la localización del EWS donde se encuentra registrado el usuario**, a partir de su identificación y contraseña.

6.5.3.4.5 Elemento Intermedio de Imagenio (EI-NGN)

La participación de este elemento en la arquitectura de NGN está relacionada **con el servicio de Videoconferencia de Imagenio**. Su función es redirigir las peticiones provenientes del elemento mediador de Imagenio (EI-CSC) a los servidores NGN del plano de servicio implicados, como el AS, Presence server ó Media server.

6.5.3.4.6 E-mail Server

Su función **es proporcionar el soporte de almacenamiento** a la solución técnica adoptada para el servicio de buzón de voz para los usuarios del servicio Centrex IP. Posteriormente el mensaje es enviado al servidor de correo que procederá a su almacenamiento local, y de ser requerido por el usuario, a su depósito en un servidor externo.

6.5.3.5 Elementos de Gestión y Monitorización

6.5.3.5.1 Ericsson Multi-Activation (EMA)

Permite **realizar la provisión de usuarios y los datos de los servicios** mediante el acceso a diferentes bases de datos desde un único punto, distribuyendo la información relevante a cada uno de los nodos implicados en proporcionar el servicio.

6.5.3.5.2 Multi-Service Network Operation Support System (MN-OSS)

Actúa **como gestor de la solución Engine Multimedia**, la realiza de forma integrada a través de los componentes comunes para la Gestión de Alarmas (Ericsson Fault Manager), Gestión de la Configuración, Gestión de Rendimiento (Analyzer), Gestión de datos de Tarificación (Ericsson Multimediation), Gestión de la Seguridad y Gestión del Software.

6.5.3.5.3 Management Console (MC)

Elemento **gestor encargado de administrar, configurar y monitorizar los Media Gateway Controller** que integran la solución de red.

6.5.3.5.4 Ericsson Multi-Mediation (EMM)

Facilita la recogida, procesado y distribución de toda la información de tarificación relevante generada por los elementos de la solución de red. En esta fase la información es proporcionada únicamente por el Aplication Server.

6.5.3.5.5 Servidor de Diagnostico

Este equipo permite **orientar a los operadores del Help Desk en la atención de las reclamaciones de los clientes**. Para ello se conecta a distintos nodos de la plataforma y obtiene de ellos información útil para el diagnóstico de incidencias. La información se solicita bajo demanda y se entrega a un sistema de tratamiento de incidencias que proporciona soporte a personal de servicio a clientes u operación y mantenimiento.

6.5.3.5.6 Subsistema de Backup

Proporciona el respaldo de la información de los sistemas mediante un almacenamiento externo. El sistema permite recuperar la información contenida en los sistemas a tres niveles, recuperación de ficheros, datos de aplicaciones y del sistema completo.

6.5.4 Conectividad de los elementos con la red IP Única

Desde un punto de vista de arquitectura de Red, **existen cuatro niveles diferenciados** en los que se incluyen los diferentes equipos que integran la solución, pudiendo cada uno de ellos pertenecer a uno o varios niveles simultáneamente. Los cuatro niveles definidos son los siguientes:

1. Un **plano de señalización o control** formado por los equipos que han de comunicarse entre sí para poder establecer las comunicaciones y prestar los servicios o facilidades soportados por la plataforma. Desde un punto de vista lógico esta subdividido en dos partes, una formada por máquinas de control y otra parte formada por máquinas de servicio.

2. Un **plano de tráfico de servicio RTP** (real time protocol), formado por elementos entre los cuales discurren los flujos de Media. Todos los elementos que están dentro de este plano, forman parte también del plano de control.

3. **Plano de acceso público de usuarios**. Lo conforman aquellas máquinas que reciben el tráfico de los usuarios, tanto de señalización como de media.

4. **Plano de gestión:** A este Plano están conectadas todas las máquinas que conforman la solución para ser gestionadas.

Todos **estos planos** que por la diferentes funcionalidades que en cada uno de ellos se prestan, **se han separado tanto física (a través de diferentes interfaces), como lógicamente (como RPV´s diferentes).**

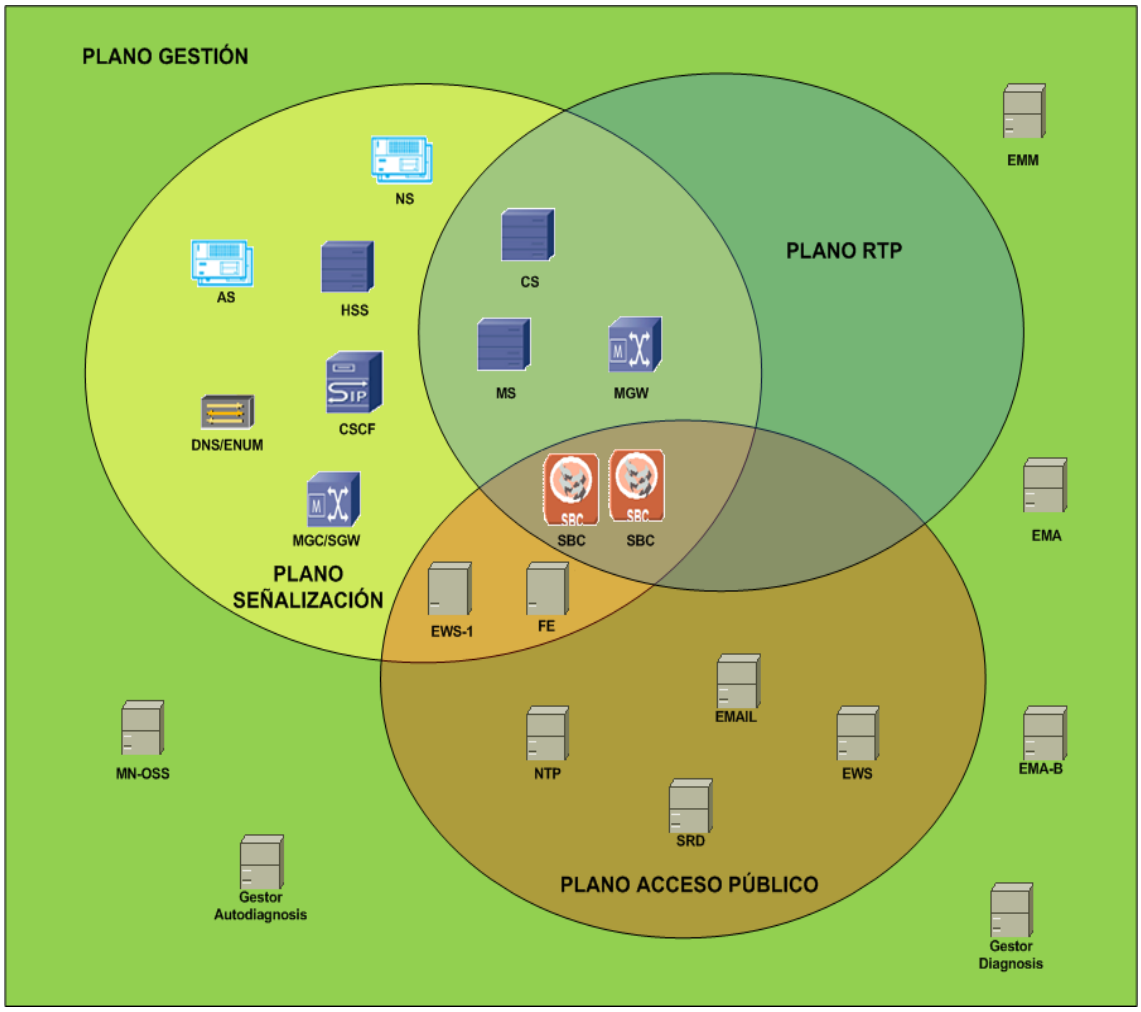


Figura 6.5.3 Esquema de funcionalidades por planos.Elaboración propia.

Los **routers de la NGN se apoyan en CA's** del Anillo Crítico. Los CA's del Anillo Crítico donde se ubican los equipos de conexión de la NGN, disponen de una pareja de Switch's NGN específica para conexiones de señalización y gestión, y para conexiones FEth de RTP (elementos Media Server's) de los elementos ubicados en ellos y poder así implementar de una manera más sencilla las políticas de seguridad mediante los FW's**. Entre los CA´s en los conmutadores de nivel 4 (L4) se define un interfaz trunk para permitir el paso de todas las VLANS correspondientes a las distintas redes que se configuran en los Centros**. Los RA´s establecen sesiones MP-BGP con estos routers reflectores de rutas.

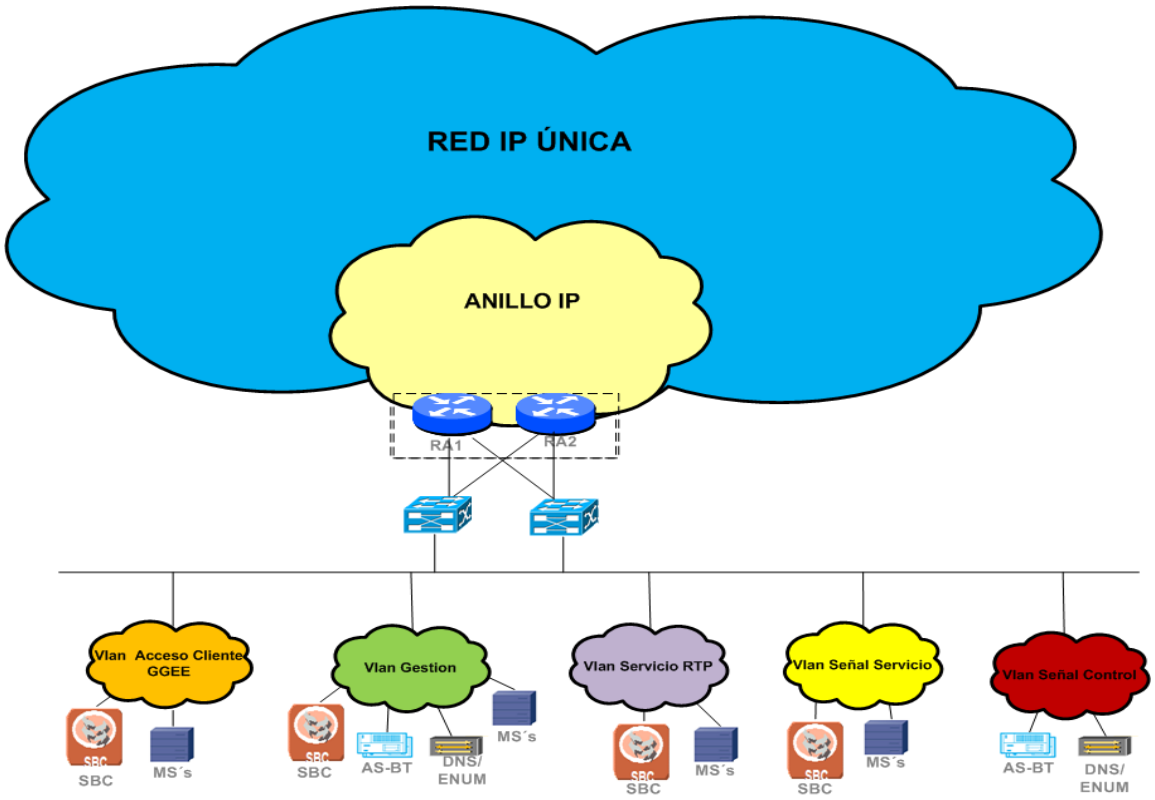


Figura 6.5.4 Arquitectura de conectividad de los elementos de la NGN con la red IP Única.Elaboración propia.

Para conocer el funcionamiento y explicación detallada del proceso de una llamada en la red NGN asi como la identificación del usuario llamante, **consultar el documento memoria_anex.pdf apartado ANEXO37.**

6.5.5 Servicios sobre la red NGN

6.5.5.1 Servicio Conexión a NGN o Accesos Primarios Virtuales

6.5.5.1.1 Descripción del servicio

El servicio de Conexión a NGN (CaNGN) **también llamado Accesos Primarios Virtuales (AAPPV / APV)** o Business Trunking es producto de la evolución de las actuales redes IP. Nace con el objeto de **integrar el tráfico de voz en la red Multiservicio de cliente**, en respuesta a las crecientes necesidades de incorporar los contenidos multimedia. La **Conexión a NGN permite el acceso de los clientes del servicio "IBERCOM IP" a la red NGN de Telefónica**, proporcionando la capacidad

de comunicación de Accesos de Voz Pública a través de tecnología IP. Es **el equivalente a un Acceso Primario, pero en IP, sin límite de canales**, que se ofrece desde la Red, y **disponible para todos los puntos de la RPV** de datos del cliente. Emula la conectividad, capacidad de comunicación y ciertos servicios de voz de las redes de voz tradicionales, soportándose en las tecnologías de VoIP. Esta **red permite al cliente interconectar sus centralitas (PABX-IP) aprovechando la RPV MPLS** existente. El Acceso Primario **proporcionará una capacidad de 10 ó 30 comunicaciones simultáneas o de cualquier agregación de múltiplos de las mismas**. Para simular las comunicaciones de voz, esto es, el canal B equivalente, se **utilizarán codecs de VoIP G.729**, que no alcanzan plenamente la calidad de voz brindada en el servicio clásico de telefonía. No obstante, NGN admite comunicaciones con codec G.711 Ley A y Ley μ.

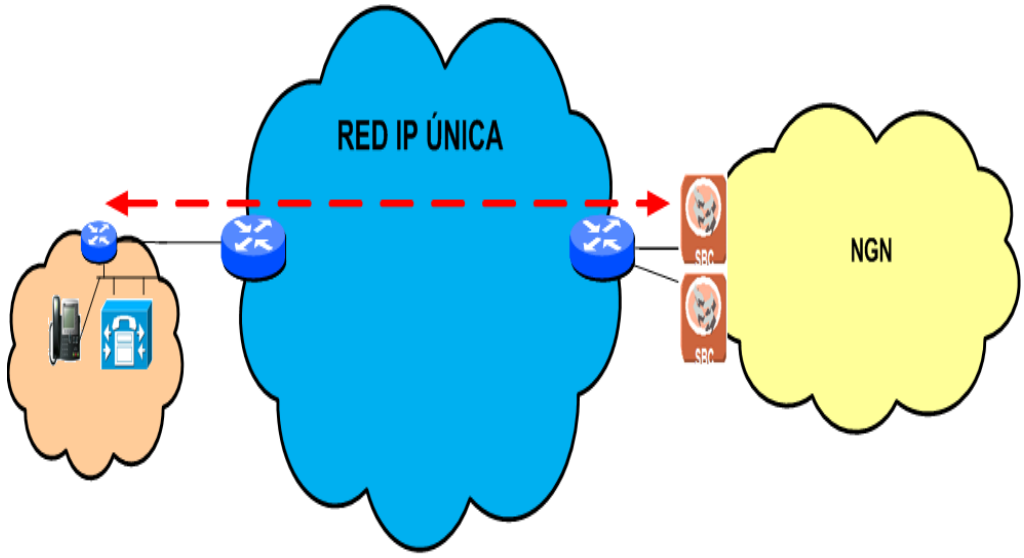


Figura 6.5.6 Esquema general del servicio AAPPV.Elaboración propia.

Uno de los requisitos de aquellos clientes que deseen contratar el servicio es disponer de una **RPV IP** (Macrolan o VPN IP) **de la red IP Única**. Esta red, al ser una red MPLS, dispone de los mecanismos de priorización adecuados para que los paquetes de datos con voz, sean transportados con los criterios de calidad que requiere la VoIp (aplicación en tiempo real). **La/s centralita/s del cliente** (normalmente serán las catalogadas dentro del servicio Ibercom Ip, Alcatel OXE, Cisco Call Manager, ASTRAA o SIEMENS) **han de tener conectividad ip con el elemento de la red NGN que hace de Gateway** de acceso hacia el resto de elementos/nodos que conforman dicha red, **el Session Border Controller (SBC).** El SBC dispone de **interfaces virtuales dentro de la misma interfaz**

física, una interfaz GigaEthernet (protocolo 802.1q).Actualmente, existe un Cluster de SBC´s dedicado al servicio BusinessTrunking, que se comporta como una sede más de la RPV de cada empresa de forma que por routing se conozcan las direcciones del SBC en el resto de sedes de la VPN, y en sentido contrario, el SBC conozca las subredes del resto de sedes de la VPN.

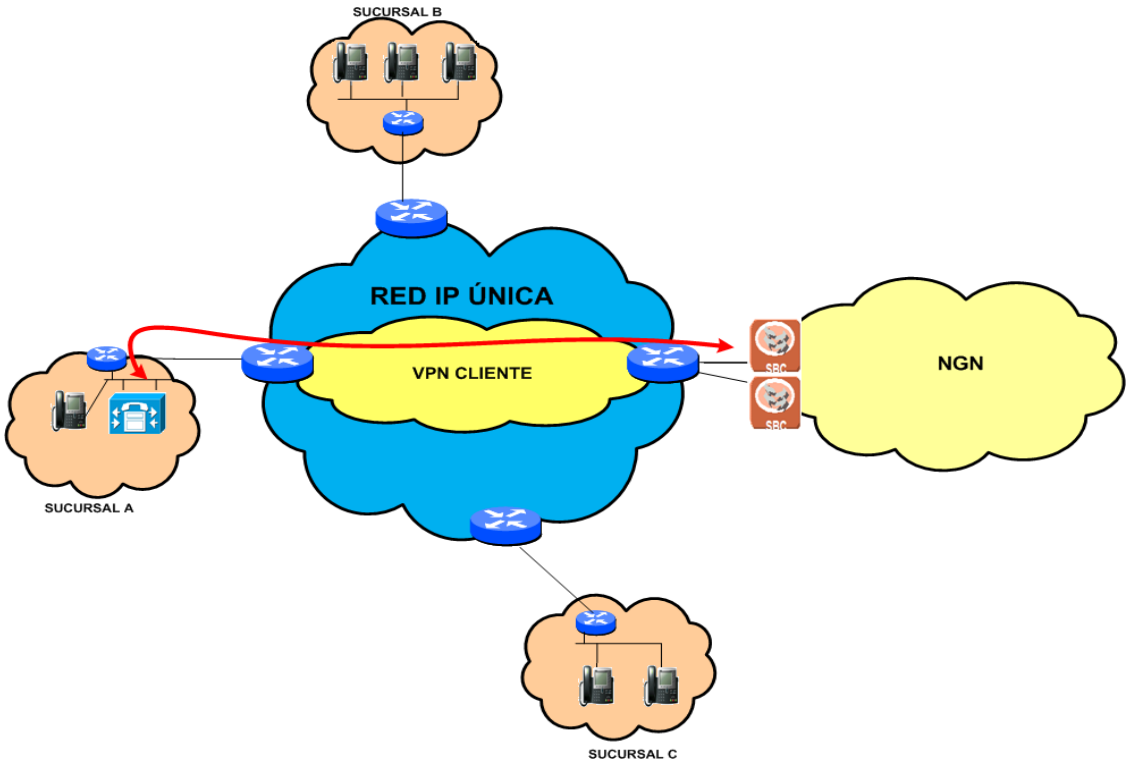


Figura 6.5.7 Conectividad sedes de un cliente con el SBC de la NGN.Elaboración propia.

Para conocer en detalle el funcionamiento del servicio AAPPVV **consultar el documento memoria_anex.pdf apartado ANEXO38.**

6.5.5.2 Servicio AUIP

6.5.5.2.1 Descripción del servicio

El Acceso Único IP (AUIP) es un servicio de conectividad que ofrece Telefónica Móviles de España (TME) a sus clientes basados en la **misma infraestructura** de que estos disponen para los **servicios de voz, datos e interconexión con la RTC (CaNGN) de que disfrutan con el servicio de IBERCOM IP**. Para ello TME contrata a Telefónica de España un servicio mayorista, denominado "Servicio de Conexión a NGN para Movistar

Corporativo" o de forma más resumida: Acceso IP para Movistar Corporativo (AIPMC). La contratación de este servicio para el cliente final lo percibe es la posibilidad de disponer de un servicio de movistar corporativo con una **conectividad IP alternativa a la basada en conexiones 2Mb**.

A día de hoy, y en el caso más general, un cliente del servicio de IBERCOM IP puede disponer de hasta tres interfaces distintas para la conexión de su PBX a la red:

- Una **interfaz IP a la red de datos IP Única de TdE** que le proporciona un servicio de VPN para sus comunicaciones de datos y de voz on-net.
- Una **interfaz de Accesos Primarios RDSI de TdE** que le proporciona fundamentalmente conectividad de voz off-net.
- Una **interfaz de Acceso Primario con la red de TME** que le proporciona acceso al servicio de Movistar Corporativo.

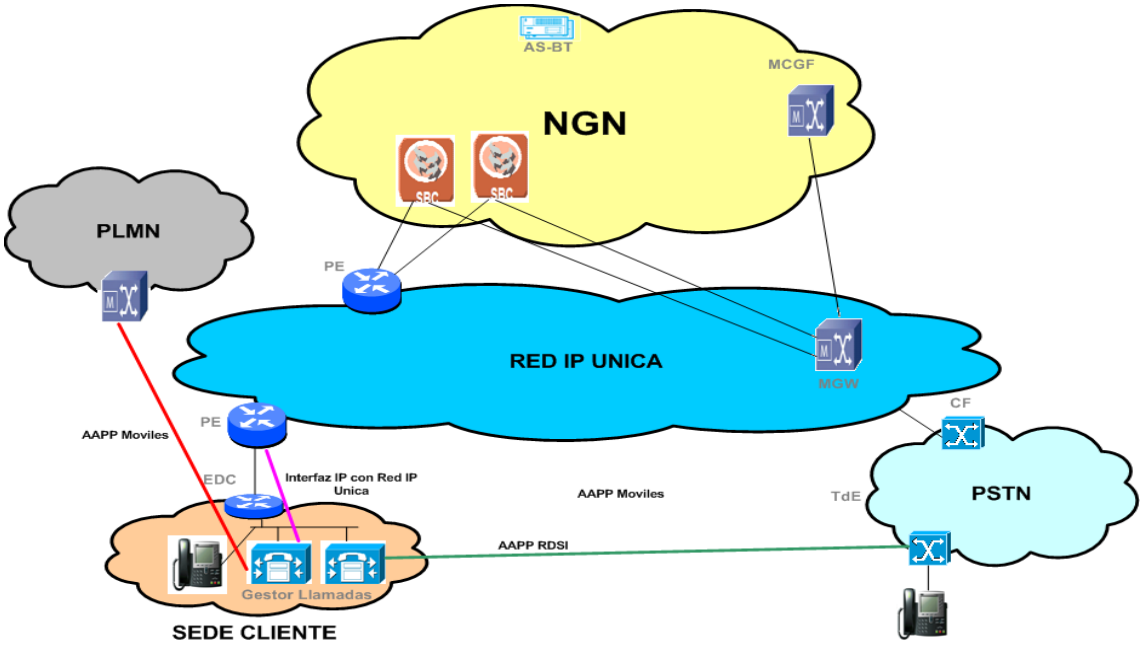


Figura 6.5.8 Arquitectura genérica inicial de clientes con Ibercom IP con tres interfaces separados.Elaboración propia.

El objetivo final es unificar **los servicios disponibles sobre las distintas interfaces ofreciéndoles a través de una solo,** permitiendo así una gestión más eficaz de los recursos, tanto para el cliente como para Telefónica.

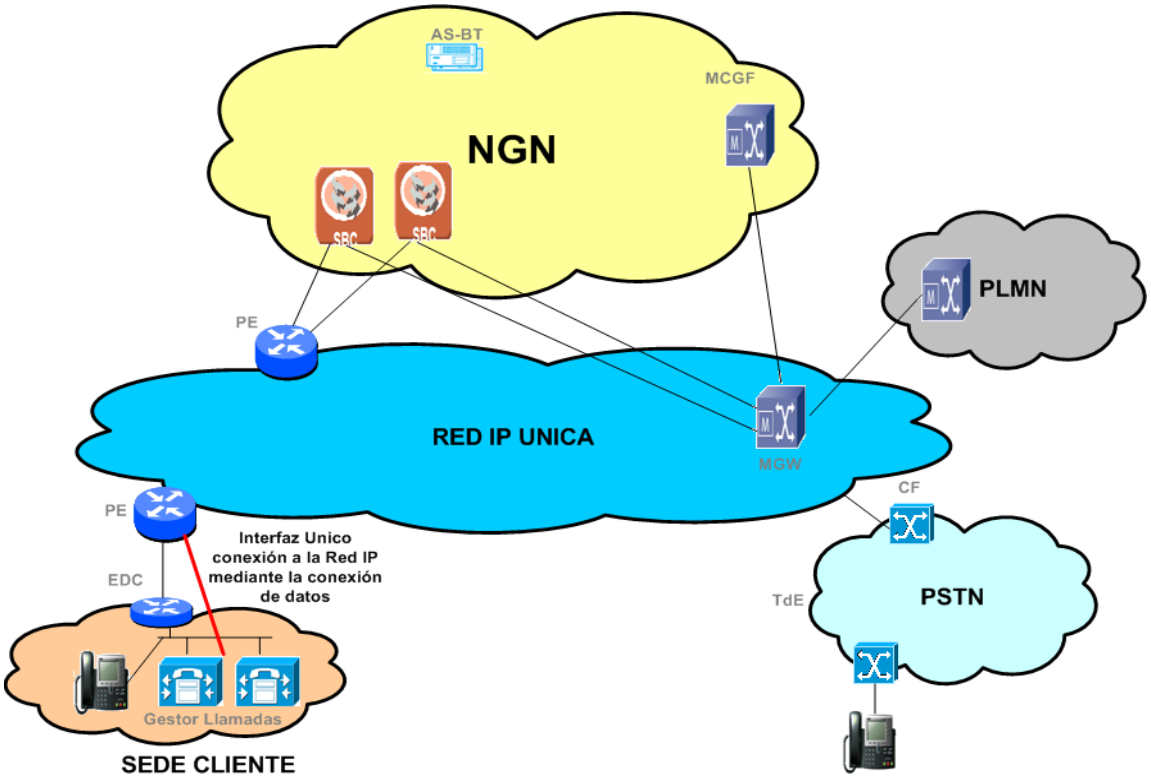


Figura 6.5.9 Arquitectura genérica final de clientes con Ibercom IP con un único interfaz hacia la red

A diferencia de lo que ocurre con las interfaces tradicionales, la **contratación de un AUIP no da lugar a la conexión de una nueva interfaz física en el domicilio** del cliente ya que una de las ventajas de este servicio es, precisamente, la **reutilización de las interfaces soporte de la VPN pre-existente** para dar conectividad al Movistar Corporativo. En el domicilio del cliente solo es **preciso reconfigurar la IP-PBX para reencaminar por el AIPMC las llamadas que de otro modo se enviarían por los AAPP** conectados con la red de TME. A diferencia del CaNGN, **AUIP simula un circuito de 2 Mbps entre TME y TdE.** La infraestructura IP es compartida por ambos servicios, **a nivel de conectividad con los SBC se diferencia el tráfico usando distintas VLAN para AUIP y CaNGN**.

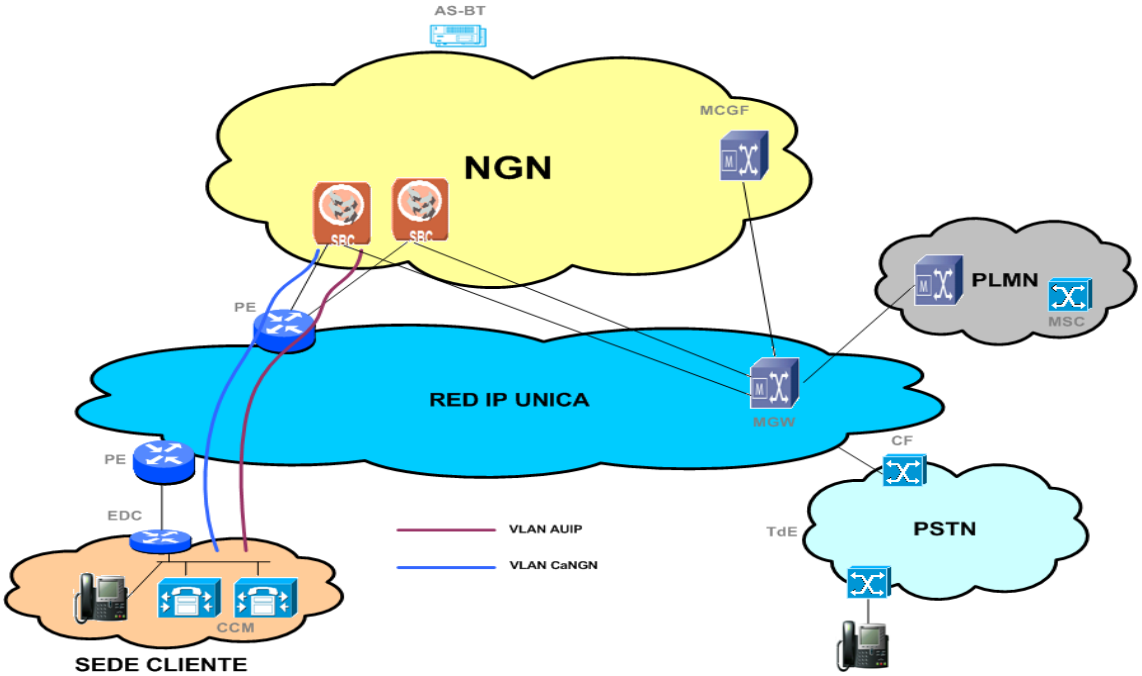


Figura 6.5.10 Conectividad con la NGN con vlanes separadas para CaNGN y AUIP.Elaboración propia.

6.5.5.2.2 Diferencias entre AUIP y CaNGN

CaNGN simula una interfaz STDP sobre tecnología IP. Esto quiere decir, que es un servicio con los mismos requerimientos funcionales y regulatorios que la RTB o la RDSI. Es una solución de conectividad que gestiona comunicaciones de voz y datos cuyos extremos se identifican mediante numeraciones públicas de carácter geográfico. El cliente lo es de TdE y esta le factura las cuotas de conexión y el tráfico. **AUIP** también simula una interfaz sobre tecnología IP, pero en este caso **no un servicio STDP, sino un circuito**. **Simula,** en definitiva, **el circuito de 2 Mb** que ahora contrata TME a TdE para poder ofrecer a sus clientes el servicio de Movistar Corporativo.

La **infrestructura IP es compartida** por ambos servicios y sin embargo en la interconexión entre la red IP Única y la NGN, **cada uno de ellos se monta sobre distinta VLAN**; así, en el caso más general, un cliente podría tener varias CaNGN conectadas a una misma RAI (Red de Acceso Ibercom) compartiendo una VLAN y, sobre otra distinta, varios AUIP. Normalmente compartirán una única red de datos y, por tanto

tendrán el mismo Administrativo de VPN identificando la misma Id_VPN. Ambas conectividades tienen sobre el caudal multimedia soportado en la red IP Única, al absorver el tráfico que antes de disponer de CaNGN y AUIP se derivaba por AAP RDSI y tramas de 2 Mb.

6.5.5.2.3 Parámetros requeridos

Si es un **alta nueva del AUIP** o por el contrario se trata solo de movimientos sobre uno ya constituido, ya que por las características del servicio, la provisión en la parte fija requiere de unos datos de carácter técnico que se generan en la red móvil, siendo preciso por tanto que la provisión en esta red se anticipe a la de aquella. Los **parámetros requeridos son**:

- **Código de cliente en la red de móviles (CC):** El código de área es un indicativo de la central IRM/MSC a la que está conectada la PABX.
- **Código de área en la red de móviles (CA):** Identifica donde está conectada la PABX dentro de la IRM/MSC.

De esto se deduce que el **conjunto CA+CC identifica de forma unívoca y exclusiva cada PABX** de cliente. En el caso del **Acceso Único IP**, estos códigos se utilizarán para identificar la IP-PABX del cliente. Se añade el:

- **Código de SCP en la red de móviles (CS):** que identifica la pareja de SCP que alojará los datos y gestionará a una PABX determinada. El SCP (Service Control Point) es el nodo de la red Inteligente de TME que facilita el acceso a la base de datos y la lógica de proceso del Servicio.

6.5.5.2.4 Conectividad red NGN con red PLMN

Los elementos de la solución **NGN implicados en la interconexión** con redes de conmutación de circuitos (en este caso PLMN), son fundamentalmente dos elementos, **la pasarela de voz o MGW y la pasarela de señalización (signalling gateway) integrada en el MGC**. Ambos proporcionan el interfuncionamiento de las dos redes, uno a nivel de tráfico de voz y el otro en el de señalización.

El **Media Gateway (MGW) es responsable del manejo de los datos multimedia recibidos** desde/hacia la red PLMN. Todos los circuitos PLMN terminan en el MGW y su tarea es adaptar la información por ellos transportada en paquetes IP. La adaptación se

realiza mediante el uso de Procesadores Digitales de Señal (DSP). **El Signalling Gateway proporciona los mecanismos portadores de interfuncionamiento para el control de la señalización (PUSI/IP – PUSI/TDM),** interconectando las entidades de control de la sesión de NGN con la red SS7 de la PSTN. Esta funcionalidad se encuentra redundada geográficamente en Madrid y Barcelona.Para conocer en detalle el funcionamiento del servicio AUIP **consultar el documento memoria_anex.pdf apartado ANEXO39.**

6.5.5.3 Servicio Ibercom IP en RED (IIPRED)

6.5.5.3.1 Descripción del servicio

El Servicio Ibercom IP en Red (IIPRED) se define como una **solución de comunicaciones multimedia** para Empresas que, aparte de funcionalidades específicas de telefonía, ofrece una amplia gama de nuevos Servicios, permitiendo realmente **la creación de una Centralita Virtual en Red**:

- Integración con directorios corporativo.
- Videoconferencia.
- Posiciones avanzadas de operadora.
- Mensajería instantánea y multimedia.
- Mensajería de voz unificada e integrada con soluciones de correo.
- Servicios de presencia.
- Agente personal.
- Soluciones de Call Center.

Se **soporta sobre una Red Privada Virtual de Datos, esto implica la contratación obligatoria de servicios MACROLAN-VPN-IP y sobre la solución de red IMS-NGN de Telefónica de España**. Con esta solución los Clientes dispondrán de un conjunto de facilidades similares a las que disfrutan los Clientes de IBERCOM IP a través de centralitas físicas. Las características fundamentales de este servicio son las siguientes:
El cliente dispondrá de la facilidad de poder **realizar y recibir llamadas de voz** cursadas sobre una Infraestructura IP, a cualquier destino, (IP, RTB, Móvil).

- Dispondrá de una serie de **funcionalidades telefónicas**, (plan privado, servicios suplementarios, servicios operadora,…).

- El servicio ofrecerá una amplia gama de facilidades tales **como plan flexible de numeración, nomadismo, acceso remoto y portal de acceso**, gestión y uso del servicio.
- Los terminales empleados en el Servicio se autoconfigurarán automáticamente descargándose el perfil de usuario así como las diferentes actualizaciones "firmware".

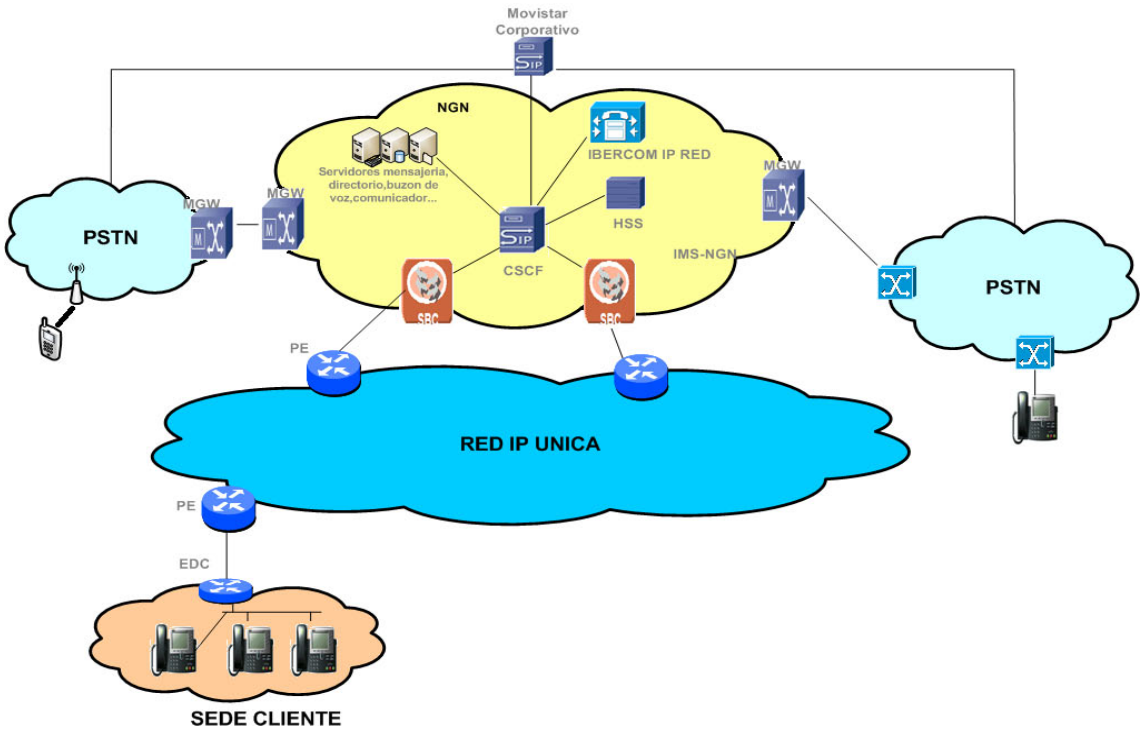


Figura 6.5.11 Arquitectura Genérica del Servicio IBERCOM IP EN RED.Elaboración propia.

La **funcionalidad básica de Ibercom IP en Red** ("stand alone") la proporciona el **AS-Broadsoft Centrex System (AS-CS)**.Por otro lado, se extendió la funcionalidad de Movistar Corporativo a usuarios del servicio Ibercom IP en red, basándose para ello en la actuación del Nodo Corporativo (AS-VPNG) como SCP de red inteligente en la red de circuitos móvil TME, y Application Server en IMS. Con ello, **el cliente tiene la percepción de que, tanto sus extensiones fijas Ibercom IP en Red, como sus extensiones móviles en el servicio "Movistar Corporativo", están todas integradas en cuanto a su facturación** y al uso del plan privado de numeración.Para conocer en detalle el funcionamiento del servicio IPRED y los elementos que intervienen en el mismo, **consultar el documento memoria_anex.pdf apartado ANEXO40.**

PARTE 2: DESARROLLO DE UN CASO PRÁCTICO PARA PUESTA EN MARCHA DE UNA OFICINA MÓVIL BASADO EN EL SERVICIO VPN-IP

1. DESCRIPCIÓN GENERAL DE LA SOLUCIÓN

Una vez explicado todos los servicios de RPVs para PYMES y Grandes Empresas que ofrecen actualmente Telefónica, voy a proceder a realizar la **configuración, montaje y puesta en marcha de un router Cisco bajo el servicio vpn-ip con acceso móvil que tiene conectividad con la red IP Única** del cliente Caja de Seguros Reunidos (CASER), es decir, estaría mapeado en la VPN de este cliente. Este equipo estaría comercializado dentro del actual portfolio de equipos del servicio VPN-IP de Telefónica.

Este tipo de equipamiento simularía la puesta en servicio de una oficina real para una gran empresa, en este caso, CASER, y que **se suele utilizar** para:

- **Emplazamientos donde Telefónica no tiene cobertura fija** (ya sea fibra óptica o par de cobre).
- **Cuando urge la apertura de una delegación y por problemas o retrasos en la provisión del servicio** no se llega a tiempo con la infraestructura fija.
- **Para empresas donde la oficina es durante un tiempo de duración determinada**, como ejemplo, podríamos tener una caseta de obra y donde el coste de tirada de líneas para darse al tiempo de baja es más costo que la solución de acceso móvil.
- Se pueda utilizar también como **respaldo de un acceso principal** (ADSL o Ibermic) en caso de caída de esta línea.

Este caso practico consistirá en **conectarnos a la VPN del cliente Caser** que tiene su vrf correspondiente en la red IP **Única a un servidor de monitorización del estado y tráfico de todas las oficinas de Caser y que se encuentra ubicada en una intranet (10.11.43.29/24) con direccionamiento privado en la oficina central de Avd. de Burgos,109 de Madrid** donde se encuentran además su DataCenter con el resto de aplicaciones, bases de datos y servidor corporativos de la empresa Caser. Conectare un portátil a la boca LAN del router y generare tráfico para que en dicho servidor de monitorización se vea como va incrementando la tasa de transferencia de bits.

Un dato imprescindible que se debe tener en cuenta **es que el direccionamiento LAN que se ponga en la oficina móvil y que se publicara por routing BGP no deberá existir en la tabla de rutas de la vrf de Caser puesto que existiría un solapamiento**

del direccionamiento y conocería la misma red desde dos oficinas provocando que problemas de conectividad. El esquema genérico de la solución a alto nivel correspondería a la siguiente figura:

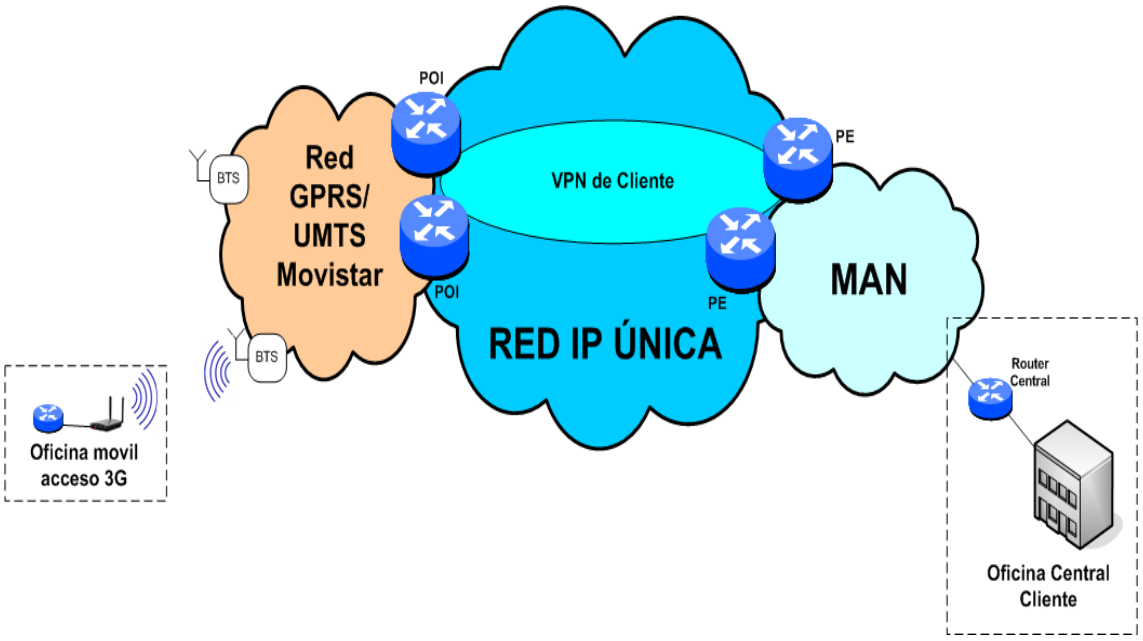


Figura 8.1.1 Arquitectura Genérica del servicio VPN-IP con acceso móvil. Elaboración propia.

2 EQUIPAMIENTO HARDWARE EMPLEADO OFICINA MOVIL

Para la puesta en marcha de la oficina móvil que tendrá conectividad con la sede central empleare el siguiente equipamiento:

- **Router cisco 887VA-M.**
- **Inyector POE** que proporcionara la alimentación al modulo de la antena 3G.
- Un modem o **antena Ethernet Teldat 3G.**
- Una **tarjeta SIM** Movistar dentro de la antena Ethernet Teldat.
- **3 cables UTP** para realizar la conectividad de la antena al router y para la conexión del portátil con el router.
- **1 portátil conectado a la LAN** de la oficina para realización de pruebas**.**

Paso a describir con más detalles las características y funcionalidades de los elementos importantes.

2.1 Router Cisco 887VA-M

El router cisco 887VA-M es un modelo que se emplea en la actualidad en diferentes servicios de RPVs de Telefónica entre ellos el de VPN-IP que es el caso que nos ocupa. **Este equipo es el CE (Customer Edge) dentro de las nomenclaturas clásicas de las VPN-IP de nivel 3 y será el encargado de establecer los túneles GRE (Generic Routing Encapsulation) contra los puntos de interconexión (POI)** que no es ni mas ni menos que los PEs que interconectan la red IP Única con la red de móviles de Telefónica Móviles.

El motivo de emplear túneles GRE es que debido a limitaciones en la red de TME, es necesaria la utilización de túneles para dar visibilidad a las redes de la sede, dentro de la VPN de cliente CASER en la red IP Única.

Mediante routing dinámico BGP, estándar del servicio vpn-ip con acceso móvil, se **anunciara el direccionamiento LAN la red configurada hacia la red IP Única para que pueda tener conectividad con cualquiera de las oficinas de Caser y con la sede central.**

Adicionalmente este **router proporcionara un cifrado a las comunicaciones para que no vaya en el claro mediante túneles estáticos IPSEC** evitando así que las transferencias realizadas desde el mismo en caso de ser interceptadas no puedan ser descifradas.

A **este router se conectara la antena Teldat UMTS y el portátil que hará de host de la parte LAN de la oficina móvil** que conectara con el servidor de monitorización de la sede central empleando la RPV de Caser. Las siguientes fotografías muestran el aspecto frontal y posterior del router cisco empleado.

Figura 8.2.1 Fotografía de la parte frontal del cisco 887 empleado como router de la oficina móvil.

Figura 8.2.2 Fotografía de la parte posterior del cisco 887 empleado como router de la oficina móvil.

Desde una temporada a la actualidad Cisco suministra las versiones de software de modo universal, es decir, que en **una misma IOS en función de las necesidades y protocolos a configurar en el equipo**, es necesario activar las licencias requeridas. En la memoria flash donde esta almacenado el archivo .bin con la versión de software se puede comprobar que es de tipo Universal.

Oficina_Movil#show flash

-#- --length-- -----date/time------ path

1 32432524 Jan 9 2013 18:09:48 +01:00 **c880data-universalk9-mz.151-4.M5.bin**

Atendiendo por tanto a la siguiente tabla del fabricante Cisco:

ADVANCED SECURITY		+ ADVANCED IP SERVICES		NO SOPORTADO
RIPv2	Soporte IEEE 802.1Q	NAT-PT	OSPF	FR Switching
DHCP (Server y Relay)	8 VLANs 802.1q	Soporte IEEE 802.1x	WCCP	FR Traffic Shaping
NAT	Auto MDX/MDI	VRF-lite	DMVPN	DLSW
HSRP	Acceso ADSL	BFD	GETVPN	XOT
CEF	CBAC (Firewall)	BGP	VRF-aware IPSEC	FRCanal B y FRCanal B 128 Kbps
Priority Queuing	Cifrado HW/SW IPSec DES, 3DES, AES	BGP Multipath	IPv6	
Custom Queuing	CBWFQ / LLQ	EIGRP	QoS avanzado (HQoS, WRED...)	
Túneles dinámicos IPSec	Soporte del estándar IEEE 802.11 Wireless			
PBR	Easy VPN	**Antena Ethernet**		

Tabla 8.2.1 Funcionalidades asociadazas a la versiones de sofware del las IOS. Elaboración propia.

En nuestro caso seria necesario activar la licencia Advance IP Service que nos permitirá configurar el protocolo de routing BGP hacia la Wan, la conectividad con la antena Ethenet y vpn que es necesario para la conectividad con los POI.

Oficina_Movil#show license

Index 1 Feature: **advipservices**

Period left: Life time

License Type: **RightToUse**

License State: **Active, In Use**

License Count: Non-Counted

License Priority: Low

Index 2 Feature: advsecurity

Period left: Life time

License Type: Permanent

License State: Active, Not in Use

License Count: Non-Counted

License Priority: Medium

Para activar la licencia basta con entrar dentro del modo configuración del terminar e incluir el siguiente mandato:

Oficina_Movil#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Oficina_Movil(config)#**license boot module c880-data level advipservices**

Se reinicia el equipo y cuando arranque, ya tendremos activada la funcionalidad Advance IP Service. Esto nos permitirá configurar BGP y VDPN entre otras funcionalidades requeridas para montar la oficina móvil.

2.2 Inyector POE

Es la fuente de alimentación externa de la antena Ethernet Teldat, que la alimenta vía un cable Ethernet UTP. Dispone de 2 puertos RJ-45 en la parte frontal y por la parte trasera la conexión a la corriente eléctrica tal y como muestra la siguiente foto:

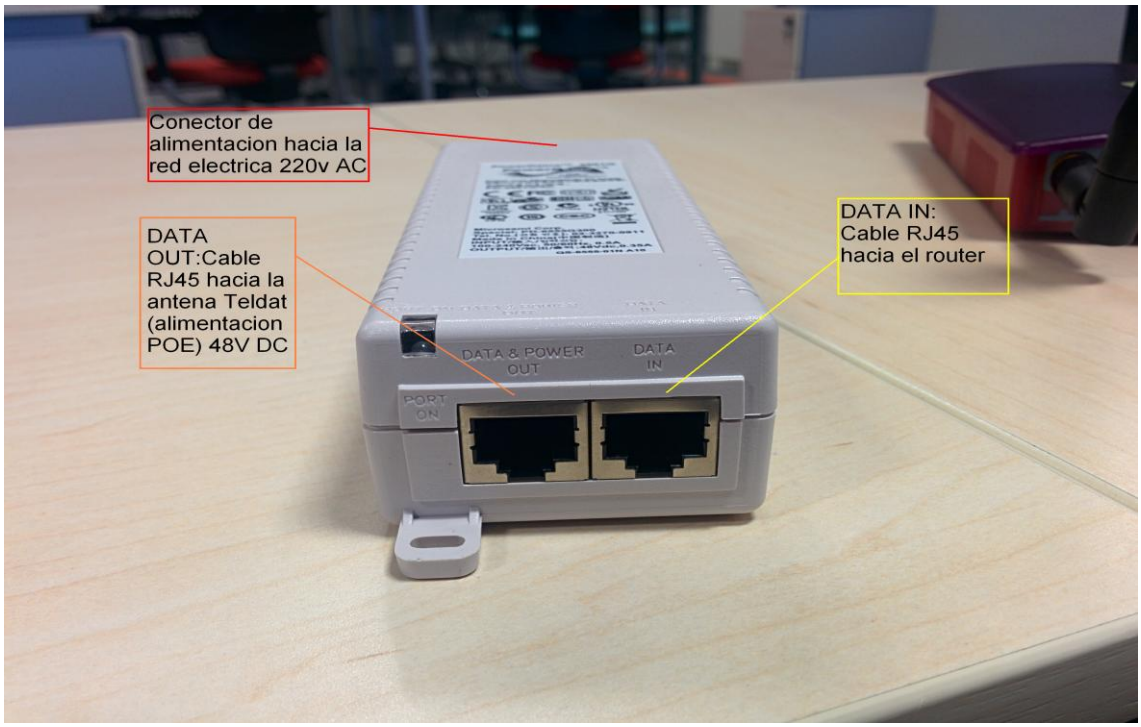


Figura 8.2.3 Fotografía del inyector POE empleado para suministrar alimentación a la antena 3G.

El puerto etiquetado como **DATA & POWER OUT** se conectara al puerto de la antena Teldat UMTS mediante un cable UTP de color Gris. Mediante esta conexión se le **proporcionara a la Antena la alimentación POE de 48 V de tensión continua**.El puerto etiquetado como **DATA IN** se conectara con el puerto 3 Fastethernet del router cisco 887 **y proporcionara la conectividad IP de la antena con el router**.El conector de la parte posterior se conectara al enchufe para proporcionar la corriente eléctrica. El esquema del conexionado final se quedaría tal y como muestra la siguiente figura:

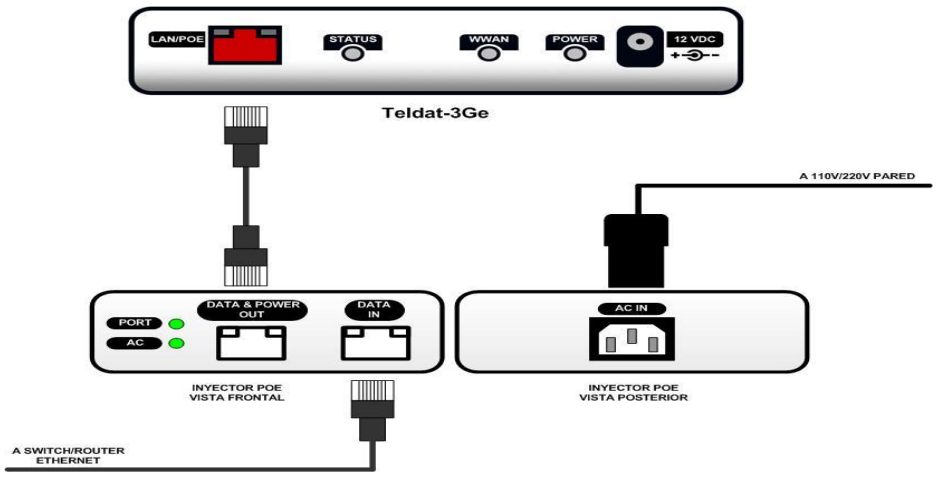


Figura 8.2.4 Esquema de conexionado del inyector POE con la antena 3G.

El uso de este inyector **POE proporcionar las siguientes ventajas**:

- **Permite instalaciones más sencillas y estéticas** al precisarse sólo de un cable a la Antena.
- **Se prescinde de la fuente externa de alimentación**.
- **Deja de ser necesario que haya un enchufe junto al módem.**

2.3 Antena Ethernet Teldat 3G

2.3.1 Descripción general de la antena

La **antena ethernet supone una mejora técnica y operativa para la puesta en servicio de RPVs** del segmento de Grandes Empresas con accesos móviles (GPRS/EDGE/UMTS/HSDPA/HSUPA) ya que antes en los routers se conectaba una tarjeta integrada equipada con una SIM pero este escenario puede plantear problemas de garantía de cobertura móvil, puesto que la antena se sitúa próxima al router, o incluso enroscada directamente a el, especialmente en instalaciones donde el router se encuentra ubicado en RACs, sótanos, estancias sin ventanas, etc. En este sentido, **la antena ethernet facilita, al utilizar cableado ethernet, la posibilidad de garantizar una mejor cobertura radio al poder situar la antena alejada del router y buscar el mejor sitio de cobertura dentro de la oficina.**

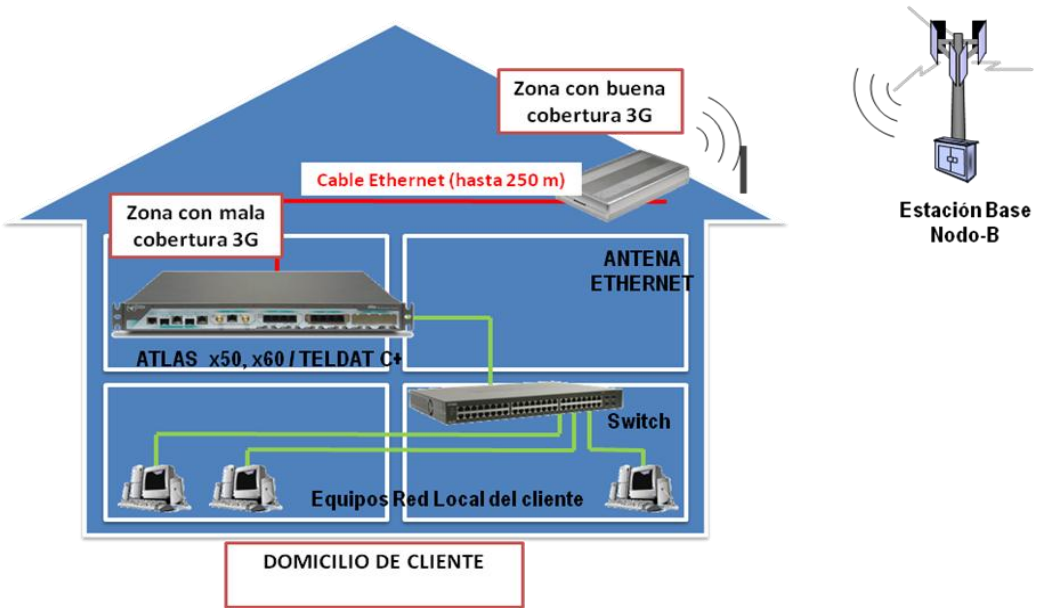


Figura 8.2.5 Esquema genérico de la red de una oficina con acceso móvil.

2.3.2 Características técnicas de la antena

La **antena ethernet es un dispositivo externo al router que soporta la funcionalidad de conectividad GPRS/EDGE/UMTS/HSDPA/HSUPA** para la configuración de escenarios de Accesos y Respaldos Móviles del servicio VPN-IP de Telefónica, la cual tratara de conectarse a la mejor red disponible, es decir, primero a HSUPA y luego descendiendo.

Figura 8.2.6 Fotografía de la antena Tedat móvil

Características del Equipo

- Dimensiones:142 x 160 x 30 mm (Largo x ancho x alto)
- Peso:450 g
- Inyector PoE externo: INPUT: 100-250V AC 50/60Hz 0.5A
  OUTPUT: 48V DC, 0.35 A
- Interface HSUPA: Modulo Sierra MC 8791V
- Interfaz Ethernet: Puerto 10/100 Base-T con autocrossover.
- Cliente: POE 802.3af (POE Class 0: 12,95W max)
- Temperatura de funcionamiento: -30ºC a 75ºC

- 2 Antenas dipolos acopables que se mueven para coger la mejor cobertura.
- 1 compartimento para la inserción de la tarjeta SIM.

2.3.3 Ubicación y parámetros de cobertura de la antena

La antena Ethernet se ubica en zonas de interior con garantía de cobertura 3,5G pudiéndose ser anclada bien a techo o a pared. En caso de tener que ubicar la antena en una situación más alejada del router, será necesario realizar una tirada de cableado Ethernet mayor. Para **buscar la mejor cobertura y el menor número de interferencias posible, se deben tener en cuenta las siguientes recomendaciones**:

- Cuando sea posible**, colocar la antena donde no existan obstáculos** físicos entre esta y la estación base, ya que degradan la señal inalámbrica. Colocar la antena por encima del nivel del suelo y orientada de forma adecuada hacia la estación base mas próxima.
- La densidad de los materiales también afecta a la antena ethernet. Se debe **situar alejada de muros de todo tipo**, mamparas metálicas, espejos, etc.
- No **colocar la antena ethernet cerca de columnas que puedan producir zonas de sombra** y que reduzcan la zona de cobertura.
- Mantenerla **alejada de otros dispositivos inalámbricos** como teléfonos, microondas, etc, ya que pueden interferir temporalmente en la calidad de la señal inalámbrica.
- **Tratar de dejar la antena fuera de RACKs que contengan equipos de comunicaciones, ordenadores, etc.** Un posible emplazamiento puede ser encima del RAC (con esto se tiene doble ventaja: se aleja la antena de fuentes de interferencia electromagnética, y se tiene un plano horizontal metálico, lo que mejora la transmisión).
- **Las antenas propiamente dichas** (los 2 dipolos acodados de color negro a enroscar en la antena ethernet**) se dejarán instaladas en posición vertical** salvo que no sea posible.
- **Los equipos con tecnología HSUPA deben quedar instalados siempre con 2 antenas.**

A continuación **se indican los valores de cobertura que se podrán encontrar en las diferentes ubicaciones que se coloque la antena**, y que permitirán determinar si la el

emplazamiento de la antena es correcto o no. Para ello paso a explicar los parámetros que determinaran si la cobertura es óptima o no:

- **Tecnología de red en uso** (Network Technology in use). Puede ser (de mejores a peores prestaciones): HSUPA, HSDPA, UMTS, EDGE, GPRS
- **Potencia de la señal recibida**. La potencia de la señal se denomina de distinta forma según la tecnología de red en uso:
  - En EDGE o GPRS:
    - **"Rxlevel"**
  - En HSUPA, HSDPA o UMTS:
    - **RSCP** (Received Signal Code Power).
- **Nivel de interferencia o calidad.**
  - En HSUPA, HSDPA o UMTS:
    - **EcIo** (Total Energy per Chip per Power Density). Su valor solo es válido con tráfico en curso.
  - El nivel de interferencia de la señal no aplica en EDGE ni en GPRS.

Con estos parámetros se determinará si el emplazamiento es válido o no. Por tanto, atendiendo a los anteriores parámetros se determina que los rangos de funcionamiento son:

1) **Para la antena funcionado en modo (2G) GPRS/ EDGE**

i) Escenario óptimo: RxLevel mayor que -75 dBm.
ii) Escenario aceptable: RxLevel entre -75 dBm y -90 dBm.
iii) Escenario inválido: RxLevel menor que -90 dBm

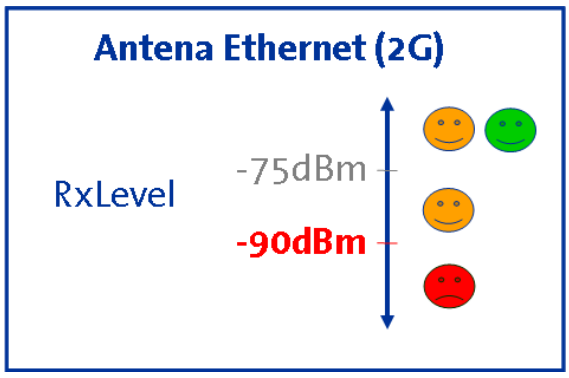


Figura 8.2.7 Tabla de valores de la potencia de la señal recibida en modo 2G.

2) **Para la antena funcionado en modo (3G) UMTS/HSDPA/HSUPA**

i) Escenario óptimo: RxLevel mayor que -75 dBm; RSCP mayor que - 85dBm; EcNO Dos o menos muestras de EcNo consecutivas con valor menor que -10dB

ii) Escenario aceptable: RxLevel entre -75 dBm y -90 dBm; RSCP entre - 85dBm y -100dBm; EcNO Tres o cuatro muestras consecutivas de EcNo menores de -10dB

iii) Escenario inválido: RxLevel menor que -90 dBm; RSCP menor que - 100dBm; EcNO Cinco o más muestras de EcNo con valor menor que -10dB

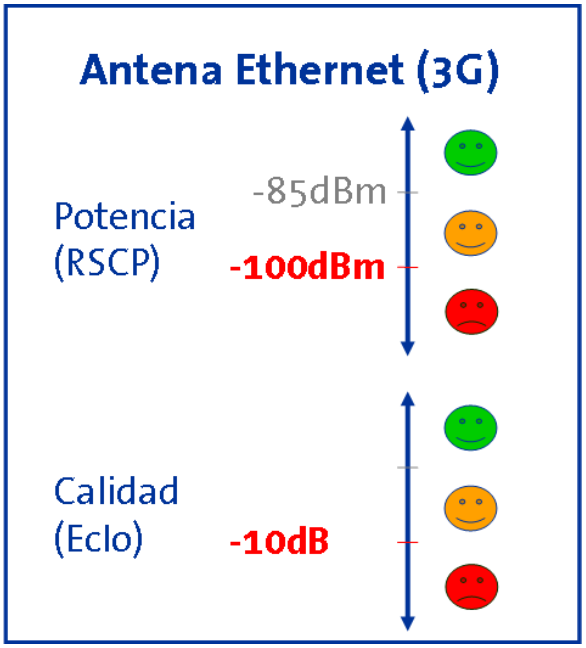


Figura 8.2.8 Tabla valores de la potencia de la señal y calidad recibida en modo 3G.

Una vez que proceda al montaje de la antena, accediendo a la IP de la antena por http se podrá comprobar mediante graficas que valores de cobertura estamos obteniendo.

2.3.4 Valores de ancho de banda

En función de la cobertura obtenida con la antena, **los valores de ancho de banda que ofrece el servicio son:**

- **GPRS:**

- Teórico: 100 kbps
- Valor Real (Orientativo): 30-40 kbps

- **UMTS**

  UMTS R99:

  - Teórico: 384 Kbps
  - Valor Real ORIENTATIVO: 384 Kbps

  HSDPA 1.8:

  - Teórico: 1,8 mbps
  - Valor Real ORIENTATIVO: 0,8-1,3 mbps

  HSDPA 3.6:

  - Teórico: 3,6 mbps
  - Valor Real ORIENTATIVO: 0,8-1,7 mbps

2.4 Tarjeta SIM Movistar

Para que la **oficina móvil funcione es necesario que se provisione una tarjeta SIM normal de MoviStar donde se configura el APN (Access Point Network) del cliente Caser que se apoya en el servicio Movistar Intranet** para que pueda acceder y tener conectividad con la VPN de la red IP Única y con el resto de las oficinas del cliente Caser. **La tarjeta SIM va insertada en un compartimento dentro de la antena Ethernet UMTS** Teldat tal y como muestra la figura.

Figura 8.2.9 Fotografía de la tarjeta SIM junto al compartimento donde se encuentra ubicada dentro de la antena Tedat.

Dos datos muy importantes que son necesarios saber de la SIM a la hora de provisionarse, son el ICC y el MSISDN:

- **ICC:** es un código de 19 dígitos (zzzzzz xxxxxx xxxxx x) que va serigrafiado sobre la tarjeta.En mi caso el ICC provisionado es **8934071100275703654.**

- **MSISDN:** es el número telefónico 6yy yyyyyy. En este caso, el número de móvil es el **676399391.**

Estos dos datos son **imprescindibles para activarlo y asociarlos en el APN del cliente Caser**. En mi caso es **acc-caja-1726.movistar.es.** Y el APN no **es mas que un código alfanumérico similar a lo que seria el número llamado en un acceso tradicional RTC/RDSI** donde el router efectúa una llamada a través del interfaz radio. Lo que se realiza básicamente que cuando la llamadaes **recibida por el equipo de la red denominado SGSN** (Serving GPRS Support Node). Dicho equipo **consulta la base de datos de abonados (HLR**: Home Location Register) para **verificar si el número llamante que originó la llamada está subscrito al APN solicitado**. Esta comprobación supone validar si el origen (número llamante) y el destino (APN) están reconocidos y registrados en la red de TME.

3 PARÁMETROS DE PROVISIÓN PARA CONFIGURAR EN EL ROUTER

En este apartado se van a describir los parámetros a configurar necesarios para la conseguir la conectividad de la oficina móvil con la el servidor de monitorización de la sede central (10.7.43.29) o con cualquier de las oficinas pertenecientes a la RPV del cliente CASER. **Los datos que a continuación son facilitados por diferentes áreas de Telefonica** (Asignación IP, Control IP, Configuracion) **durante la provisión del circuito de acceso móvil**. En este caso los datos suministrados para hacer funcionar la oficina móvil son:

<APN_Cliente> -> **acc-caja-1726.movistar.es**. APN dentro de la red TME para Caser.
<Password> -> **caja1726** . Password asignada a la oficina móvil para realizar la autenticación en el radius una vez efectuada la llamada desde el router.
<identificativo_unico> 1726_sucursal156. Identifica de manera única a la oficina móvil. También denominado ID_Sucursal. Es utilizado en el radius para identificar desde que acceso se esta realizando la llamada.

<POI_Principal> -> NMAMNOR3. Este es el POI o PE principal de la red IP Única contra el que se establecera el tunel GRE principal la oficina móvil.

<POI_Principal> -> NMABLLA3. Este es el POI o PE backup de la red IP Única contra el que se establecerá el tunel GRE backup la oficina móvil. Este cursara el tráfico en el caso de caída del tunel principal.

<IP_EDC_TUNEL> -> 10.148.18.193. La dirección IP asignada al interfaz radio de nuestra sede. Para el servicio es necesario establecer un par de túneles GRE (túnel principal y túnel de backup) entre el EDC y los POIs designados para la oficina móvil. En el EDC estos túneles se crearán tomando siempre como dirección origen la IP asignada al interfaz de radio, es decir, la ip 10.148.18.193

Figura 8.3.1 Esquema de red genérico del servicio vpn ip con acceso móvil sobre la utilización de la IP EDC TUNEL en el router. Elaboración propia.

<IP_POI_TUNEL_PRAL> -> 172.19.136.61 Dirección IP Wan de destino asignada en el POI NMAMNOR3 para montar el túnel GRE principal.

<IP_POI_TUNEL_BCK> -> 172.19.136.129 Dirección IP Wan asignada en el POI NMABLLA3 para montar el túnel GRE de backup.

A estos interfaces de túnel GRE que se van a crear contra entre la oficina móvil y los POI tienen que asignarle un direccionamiento WAN:

<IP_Wan_EDC_Tunel_Pral> -> 10.21.34.34 Dirección IP asignada en la oficina móvil al interfaz de túnel principal

<IP_Wan_POI_Tunel_Pral> -> 10.21.34.33 Dirección IP asignada en el POI NMAMNOR3 al interfaz de túnel para la oficina móvil

<IP_Wan_EDC_Tunel_Bck> -> 10.21.34.50 Dirección IP asignada en la oficina móvil al interfaz de túnel backup

<IP_Wan_POI_Tunel_Bck> -> 10.21.34.49 Dirección IP asignada en el POI NMABLLA3 al interfaz de túnel para la oficina móvil.

Por tanto, **cada interface de túnel definido, es como una conexión punto a punto entre la oficina móvil con acceso GPRS/UMTS y los POI por eso las anteriores IPs con una mascara /30 será suficiente.**

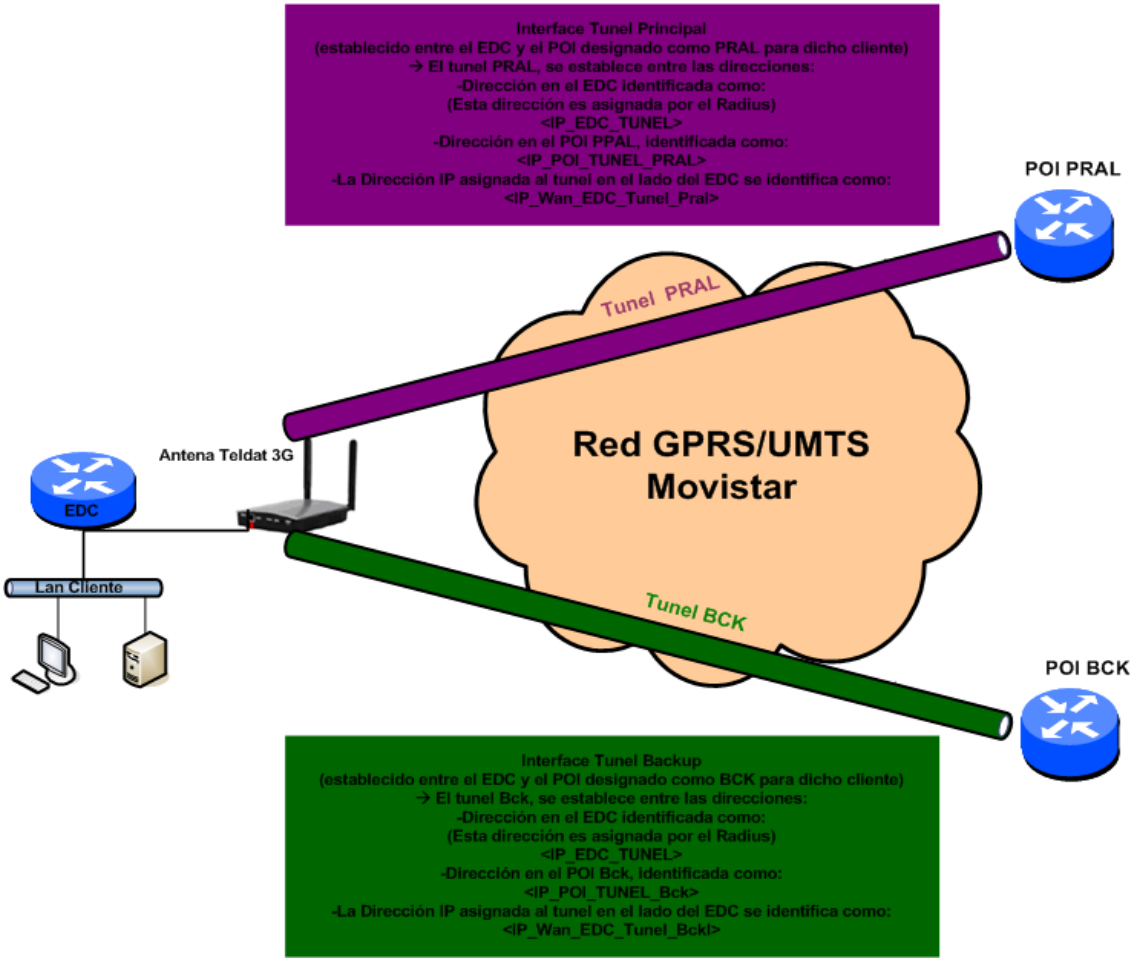


Figura 8.3.2 Esquema de red sobre la utilización de las IPs denominada IP Wan EDC túnel. Elaboración propia.

<Red_LAN_Oficina_Movil> -> 10.22.200.0 Red LAN utilizada para el direccionamiento de los equipos conectados al router de la oficina móvil y que dicho direccionamiento no tiene solapamiento dentro del plan de direccionamiento privado de la RPV del cliente CASER.

Los parámetros adicionales que se derivan del montaje de la antena Ethernet Teldat UMTS se basan en el montaje de una red LAN /30 la cual será utilizada para que la antena tenga conectividad con el router y pueda descargarse por DHCP los parámetros de configuración de IP y del firmware.

<RED_LAN_ANT-EDC> -> 10.100.100.0/30 Red LAN asociada a la conexión exclusiva entre el EDC y la Antena Ethernet. Esta red no se anunciara a la WAN, es de ámbito local. Y con una /30 será suficiente para gestionar el direccionamiento entre router y antena.

<IP_EDC-LAN_ANT-EDC> -> 10.100.100.1 Dirección IP del EDC en la LAN exclusiva de conexión entre el EDC y la Antena Ethernet.

<IP_ANT-LAN_ANT-EDC>-> 10.100.100.2 Dirección IP de la Antena-Ethernet en la LAN exclusiva de co-nexión entre el EDC y la Antena.

<ID_VLAN_Ant-Eth> -> 19. Vlan Dedicada para la comunicación entre el Router y la Antena. Para dicha Vlan el identificativo que he utilizado es el 19 y no utilizare encapsulación 802.1Q puesto que en el puerto Fa3 del router solo ira conectada la antena y es necesario realizar múltiplexación de vlanes.

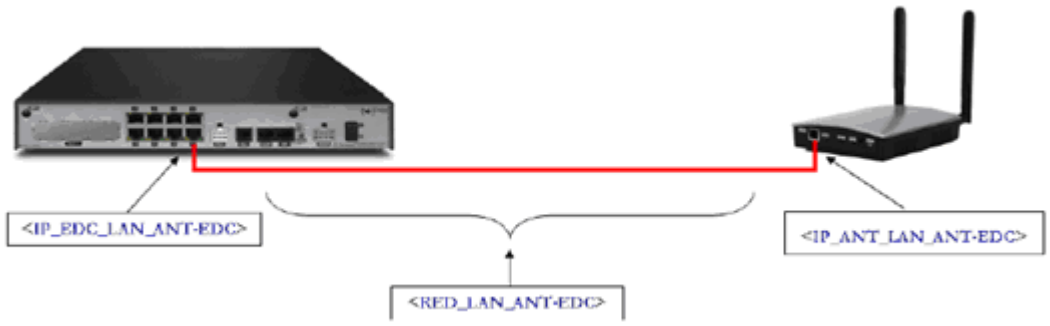


Figura 8.3.3 Esquema de red para explicar donde se emplean las IPs LANs de la antena. Elaboración propia.

Como he indicado anteriormente, **se requiere un servidor DHCP en el router, que es el encargado de facilitar los parámetros IP necesarios tanto para el correcto establecimiento del túnel L2TP**. Los parámetros a configurar son los siguientes:

<antenna>, es la cadena de validación DHCP. La Antena Ethernet 3G sólo admite parámetros DHCP recibidos de un servidor que contenga la cadena "antenna".

<**routertype=generic>**, especifica el modo de operación que permite a la Antena Ethernet 3G operar y ser gestionada de manera genérica.

<**apn=acc-caja-1726.movistar.es>** especifica el Punto de Acceso a la red 3G (APN).

<**rxtimeout=360>**, activa la detección pasiva de caída de servicio 3G por tiempo de inactividad. 360 segundos es el tiempo que puede estar sin recibir datos entrantes tras el último paquete enviado por su interfaz 3G para no lanzar el proceso de desconexión. Vencido este tiempo sin recibir datos entrantes, se reinician los interfaces de comunicación.
<**regdenied=1>**, Si su valor es 0, transcurridos un número determinado de intentos de registro en la red la antena entraría en estado idle. Por el contrario, cuando su valor es 1, continúa intentándolo de forma ininterrumpida.
<pin= >, especifica que el PIN esta deshabilitado en la tarjeta SIM.

Para realizar la monitorización del trafico que pasa por los interfaces de la oficina móvil desde el **servidor de monitorización (10.11.43.29) que se encuentra en la intranet de la sede central, es necesario definir una loopback** para que dicho servidor realice consulta de snmp a ese interfaz:

<IP_SNMP_Monitorizacion> -> 172.29.29.200. Esta IP es la que atacara el servidor de snmp para realizar consultas de monitorización.

En un acceso móvil**, el tráfico que viaja** contra la estación base y los POI de la red IP **viaja en claro, es decir, no esta cifrado**, por lo que si un atacante interceptase el tráfico generado podría ver y analizar que tipo de trafico esta pasando suponiendo un riesgo y una vulnerabilidad de la información. **Para ello voy a configurar túneles IPSEC estáticos contra los equipos centrales WAN de la sede central**. Para configurar estos túneles es necesario definir una IP de peer de establecimiento del túnel.

<IP_CIFRADO> -> 10.95.246.200. IP empleada para establecer el túnel IPSEC contra la sede central y cifrar las comunicaciones.

4 ESQUEMA Y EXPLICACION DETALLADA DE LA INFRAESTRUCTURA GLOBAL

En el siguiente esquema quedan reflejados los elementos de la red que intervienen con su direccionamiento asignado para el montaje y funcionamiento de la oficina móvil dentro de la RPV de Caser en la red IP Única y que proporcionara conectividad con el servidor de monitorización de la sede central. Se han suprimido ciertos equipos de red del esquema, como son los equipos pertenecientes a la red GPRS/UMTS para no complicar la explicación del servicio en cuestión.

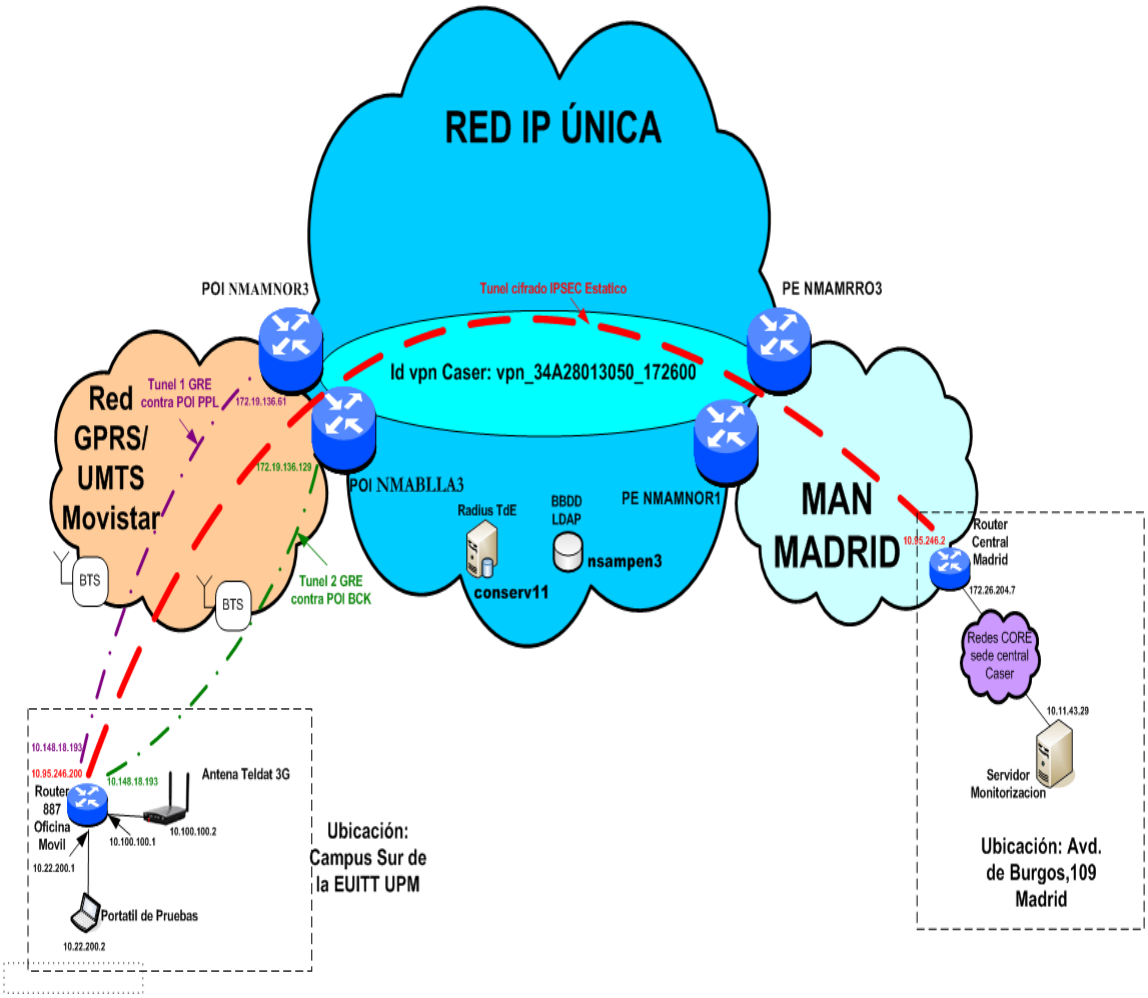


Figura 8.4.1 Esquema de red global de la infraestructura que intervienen para que la oficina móvil alcance el servidor de monitorización. Elaboración propia.

Para que la **oficina móvil pueda tener conectividad con la RPV de Caser en la red IP se apoya en el servicio Movistar Intranet a través de la red móvil GPRS/UMTS de Movistar**. El Servicio **Movistar Intranet proporciona la solución de acceso a la red IP Única a través de la Red Móvil (GPRS/UMTS**). Además **proporcionará la autenticación de los accesos**, comprobando que el numero llamante (**676399391**) esta asociado al APN de Caser (**acc-caja-1726.movistar.es). Esta asociación es necesaria para incluir dichos accesos de cliente en la RPV de Caser** creada en la Red de móviles.

El router Cisco 887 de la oficina móvil gestiona la antena ethernet 3G mediante un interfaz de tipo virtual-ppp, es decir, la comunicación con la antena ethernet 3G viaja sobre una conexión PPP de tipo client-initiated. La conexión PPP se transporta sobre un túnel L2TP pseudowire establecido entre los dos equipos. Esta aproximación permite al router ofrecer sobre la antena ethernet 3G prestaciones funcionales, de configuración y de monitorización.

La llamada realizada desde el interfaz radio de la antena Teldat 3G es **recibida por el equipo de la red denominado SGSN** (Serving GPRS Support Node). Dicho equipo **consulta la base de datos de abonados (HLR**: Home Location Register) para verificar si el número llamante que originó la llamada está subscrito al APN solicitado.Una vez completada la primera verificación, el **SGSN** que ha registrado la llamada **progresa la conexión hasta el GGSN** correspondiente. En concreto el SGSN que registra la llamada establece un **túnel GPRS (GTP: GPRS Tunneling Protocol) contra el GGSN** que actúa como pasarela.

El GGSN que recibe la conexión **negocia el establecimiento de una conexión Punto a Punto (PPP) con el router con acceso GPRS/UMTS**. En la primera parte de la negociación PPP: **LCP (Link Control Protocol), se determina básicamente el tamaño de trama (MRU: Maximum Reception Unit) y el protocolo a través del cual el router va a intercambiar las claves de acceso (PAP ó CHAP).** Tras efectuarse la negociación inicial el equipo GGSN consulta al servidor Radius **(Conserver11)** para validar los datos de usuario (**1726_sucursal156)** y password **(caja1726)** indicados por el router. Para ello el Radius Conserver11 consultara en la BBDD almacenado en el equipo **nsampen3** mediante LDAP que los anteriores usuarios y password están dados de alta.

Una vez validado el acceso se inicia la **segunda parte de la negociación PPP (IPCP: IP Control Protocol), donde se determinan los parámetros del nivel de red asociados a la conexión**. En concreto en nuestro caso **el GGSN le indica al router 887 la dirección IP WAN (10.148.18.193) que debe emplear. Los servidores Radius previamente han indicado al GGSN qué IP WAN debe asignar pues esta viene almacenada en la BBDD de LDAP**. **La asignación de IP es estática**, es decir a una sucursal siempre se le asignará la misma dirección IP WAN y dicha IP es la que aparecerá en el interfaz virtual-ppp1.

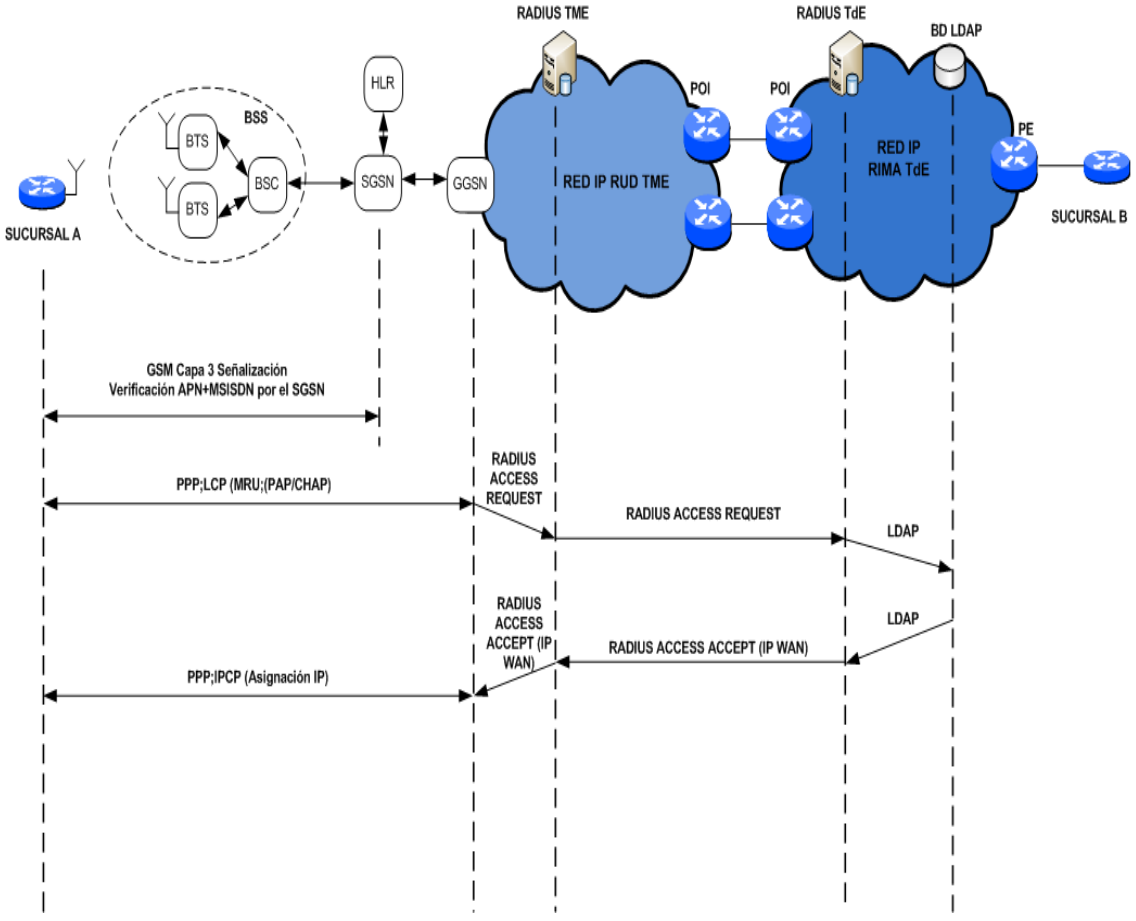


Figura 8.4.2 Proceso de establecimiento de conexión GPRS/UMTS. Elaboración propia.

Una vez conseguida la conectividad de la oficina móvil con acceso UMTS y los POIs (NMAMNOR3 y NMABLLA3) de la red IP Única, todo ello mediante las arquitecturas definidas con anterioridad, **se debe conseguir la conectividad de la oficina móvil tenga comunicación con el resto de sedes de la VPN de Caser.** Por ello, debido a limitaciones en la red de móviles, es necesaria la utilización de túneles para dar visibilidad a las redes de la sede, dentro de la VPN de Caser de la red IP Única. **Por las prestaciones de los routers y requerimientos de Telefonica, los túneles empleados para conectarnos con los POIs son túneles GRE (Generic Router Encapsulation).**

GRE es un protocolo que puede encapsular una amplia variedad de tipos de protocolos diferentes dentro de túneles IP, creando una red punto a punto entre el router de la oficina móvil y los POIs. El esquema virtual de la oficina móvil con los POI seria el siguiente:

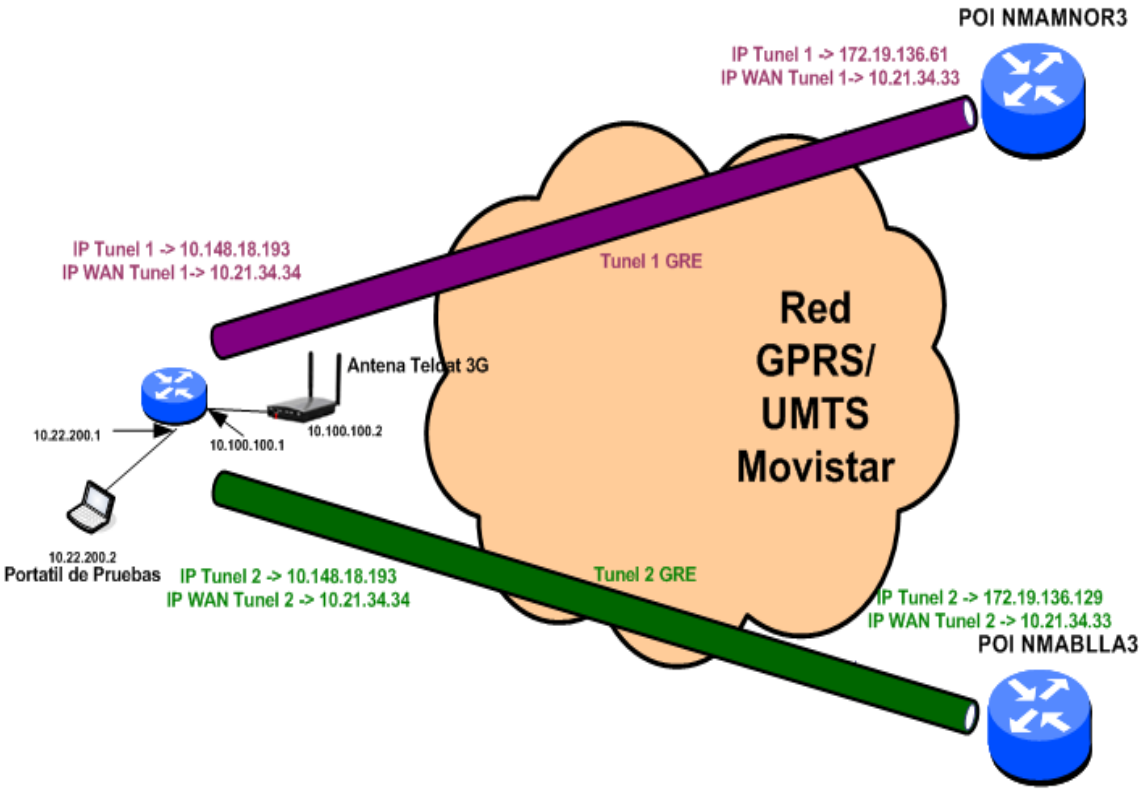


Figura 8.4.3 Esquema de red de los túneles GRE con los POIs. Elaboración propia.

Como he explicado anteriormente la IP Túnel del router de oficinas es asignada estáticamente por el radius una vez que se ha valido. **Las IP Wan son las pertenecientes**

a los interfaces túnel es como si simulase una conexión pto a pto entre el router 887 y los POIs, por tanto, con direccionamiento con mascara /30 será suficiente para asignar a los equipos implicados en la comunicación.GRE toma un paquete ya existente, con su encabezado de capa de red, y le agrega un segundo encabezado de capa de red, lo que implica que el paquete que se envía a través del túnel es de mayor longitud por lo que puede ocurrir que esté excediendo la longitud permitida en la interfaz túnel.

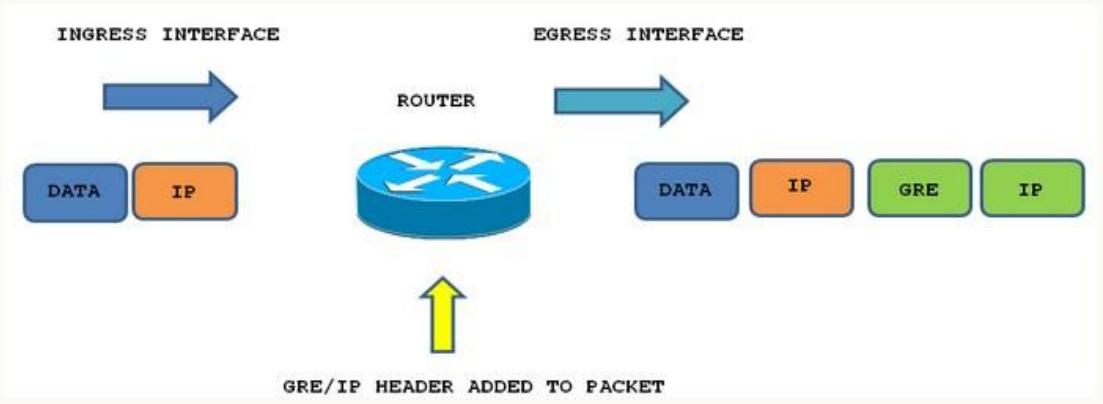


Figura 8.4.4 Esquema del paquete IP antes y después del tunel GRE. Elaboración propia

La MTU máxima que puede transitar por la Red de móviles sin ser fragmentado el paquete IP, es de 1500, por lo que, **para que se evite la fragmentación se adapta la MTU de los túneles en 1476**.Como los túneles GRE son estáticos, no existe señalización del estado del interface de túnel, por lo que para detectar su caída se precisa de algún mecanismo adicional, en este caso se utiliza el routing dinámico **para detectar las caídas de los túneles, concretamente routing BGP debido a que se generaran 2 túneles con los POIs para conseguir la redundancia de la conexión** de la oficina móvil en caso de caída de uno de los túneles.

Adicionalmente para que el servidor de monitorización de la sede central de Caser tenga conectividad con la LAN de la oficina móvil **(10.22.200.0/24) se anunciara dicha red por BGP hacia la WAN por los túneles GRE. Los POIs que reciben esa red por BGP lo exportara en la vrf de la red IP Única del cliente Caser (vpn_34A28013050_172600) con la ayuda de los mecanismos de RT (3352_172600) y RD (3352_172600) de la VPN que pertenece Caser.**

Para dotar de **cifrado al tráfico** que se cursa por acceso 3G y evitar que vaya el flujo de datos en claro, se **configurara un túnel IPSEC estático entre el router de 887 de la oficina móvil y el router central** de la sede de Madrid de Caser. **La función de IPSEC es asegurar las comunicaciones sobre IP autenticando y/o cifrando cada paquete IP**. El **cifrado** que se configurara será en **modo túnel, es decir, todo el paquete IP (datos más cabeceras del mensaje) es cifrado y/o autenticado.** Por tanto, debe ser entonces encapsulado en un nuevo paquete IP para que funcione el enrutamiento. El modo túnel se utiliza para comunicaciones red a red o comunicaciones ordenador a red u ordenador a ordenador sobre una red insegura. La siguiente figura especifica la topología IPSEC que se montara entre la oficina móvil y el router central.

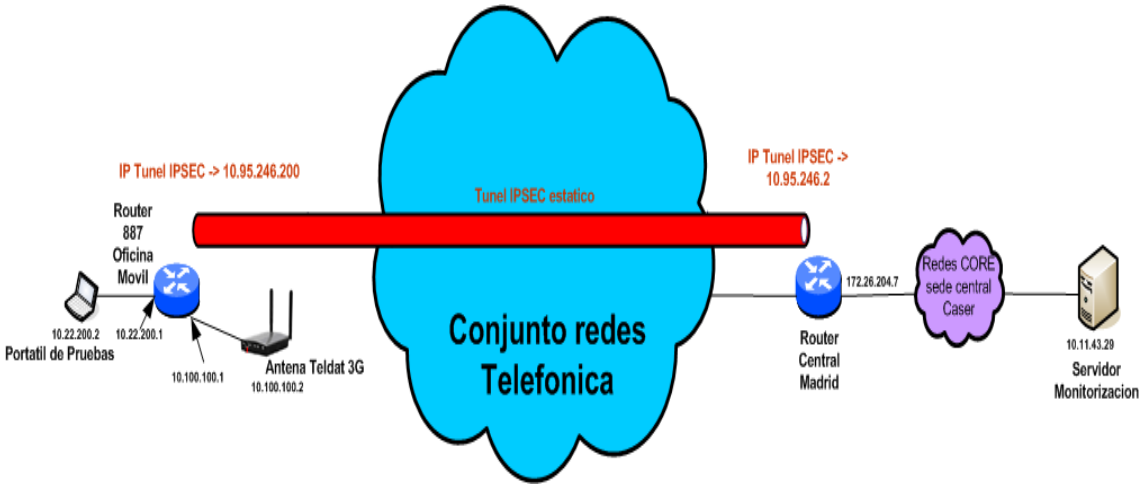


Figura 8.4.5 Esquema de red del túnel IPSEC entre la oficina móvil y el router central. Elaboración propia

Las IP tunel IPSEC se definirán en ambos routers en una interfaz de loopback y serán las IPs peer que se definirán para montar el túnel y que irán en las cabeceras del datagrama IP ya que el cifrado será en modo túnel. Para establecer el túnel es requisito que ambos routers conozcan las IPs túnel IPSEC por tanto estas se anunciaran hacia la WAN por routing BGP. El criterio del tráfico que se cifrara será el que vaya con origen la red 10.200.22.0/24 a la red 10.11.43.0/24 y viceversa. El router 887 que recibe el tráfico desde la LAN y verifica que cumple las condiciones especificadas para que el tráfico sea cifrado (IP Origen o destino o puerto TCP origen o destino) desencadena las siguientes fases:

1. **Negociación.** Permite el reconocimiento y aceptación de los equipos origen y destino como equipos capaces de cifrar, desencadena la negociación de la sesión IKE.
2. **Sesión IKE.** Mediante este protocolo se negocia la asociación de seguridad entre 2 entidades (SA de IPSec) permitiendo:
   a. Negociación entre los equipos origen y destino del túnel cifrado de los algoritmos y tipo de claves a utilizar
   b. Autentificar que los equipos origen y destino del túnel cifrado son los que realmente son.
   c. Gestionar las claves tras haber sido aceptadas.
   d. Intercambio de claves de forma segura.
3. **Sesión IPSec.** Define el método de cifrado de los paquetes de datos, así como la información con la que se completa el paquete para permitir el control de la confidencialidad, integridad y autenticidad.

Por último la parametrizacion que llevara el túnel IPSEC será la siguiente:

1. Los valores para la **sesión IKE son:**

- Algoritmo de cifrado: **3DES**
- Algoritmo de autenticación (hash): **MD5.**
- Negociación Diffie-Hellman: **Grupo 1.**
- Tiempos de vida (lifetimes): **6 horas**.
- Proceso de autenticación: **Secreto compartido**
- Keepalive: Cada **60 segundos** y perdida de **2 consecutivas**
- Clave: **Secreto Compartido**

2. Para la **sesión IPSEC son:**

- Algoritmo de cifrado: **esp-3des** combinado con **esp-sha-hmac**
- Tiempos de vida (lifetimes):**5horas**
- Modo de operación: **Modo Túnel.**

5 CONFIGURACION ROUTER 887 OFICINA MOVIL

5.1 Configuración del interfaz LAN de conexión con la antena UMTS

```
interface Vlan19
 description Vlan Conexion ANTENA_UMTS
 ip address 10.100.100.1 255.255.255.252
!
interface FastEthernet3
 description Conexion Antena Ethernet UMTS
 switchport mode access
 switchport access vlan 19
 no ip address
!
```

La antena ira conectada por cable UTP al puerto FastEthernet3 del router al cual se asocia la vlan 19 y se configura la vlan 19 de nivel 3 con el direccionamiento de la red 10.100.100.0/30

5.2 Servidor DHCP

```
service dhcp
ip dhcp pool ethant
 host 10.100.100.2 255.255.255.252
 client-identifier 7465.6c64.6174
 next-server 10.100.100.1
 option 43 ascii "antenna&routertype=generic&pin=&apn=acc-caja
1726.movistar.es&rxtimeout=360&regdenied=1"
 default-router 10.100.100.1
!
```

El **servidor DHCP del router Cisco, suministra a la Antena Ethernet 3G sus parámetros IP,** y además también **parámetros de acceso al servicio 3G** y otros parámetros de control de acceso **mediante la opción 43 de DHCP**. El comando client-identifier 7465.6c64.6174 especifica el identificador de cliente, deforma que el servidor DHCP del router sólo acepte peticiones de la Antena Ethernet 3G. La cadena hexadecimal de este parámetro es "74656c646174", cuyo valor ASCII es "teldat".

Respecto a la configuración **empleada de opción 43 de DHCP es debido a que la antena teldat UMTS solo admite como parámetro la cadena de validación DHCP ("antenna").** En la cadena ASCII se especificar parámetros tanto de control de acceso al servicio DHCP. La explicación de cada uno de los parámetros ya esta explicada en apartados anteriores.

5.3 Interfaz Virtual PPP1

```
interface Virtual-PPP1
 ip address negotiated
 ppp pfc local request
 ppp pfc remote apply
 ppp acfc local request
 ppp acfc remote apply
 ppp chap hostname 1726_sucursal156@vpn-mv-acc-caja-1726
 ppp chap password caja1726
pseudowire 10.100.100.2 1 pw-class pwclass1
!
```

El router Cisco gestiona la Antena Ethernet 3G mediante un interfaz virtual, es decir, **la comunicación con la Antena Ethernet 3G viaja sobre una conexión y transporte del protocolo PPP**. La **conexión PPP se transporta sobre un túnel L2TP pseudowire que simula un circuito de nivel 2** establecido entre los dos equipos. Es decir, este interfaz virtual agrega la encapsulación de nivel 2 a los paquetes de nivel 3, permitiendo que se realice el negociado y autenticación de la sesion PPP con el GGSN de

la red 3G. **Esta aproximación permite al router ofrecer sobre la Antena Ethernet 3G prestaciones funcionales, desconfiguración y de monitorización equivalentes a las ofrecidas sobre sus interfaces 3G internos.**

El mandado **ip address negociated quiere decir que una vez que se autentique la conexión en el Radius, este, el suministrará que IP que debe llevar este interfaz 10.148.18.193**. La dirección destino del túnel se corresponde con la que el servidor DHCP, es decir el router, le asigna a la Antena Ethernet que seria la IP 10.100.100.2

5.4 Tunel L2TP con antena UMTS

```
vpdn enable
!
l2tp-class l2tpclass1
hidden
hello 10
retransmit retries 5
!
pseudowire-class pwclass1
encapsulation l2tpv2
protocol l2tpv2 l2tpclass1
ip local interface Vlan19
!
```

Se activa la funcionalidad VPDN del router Cisco 887. A continuación, se establecen los parámetros del túnel L2TP. **Por último se crea una clase pseudowire para utilizar la versión 2 del protocolo L2TP y definir el interfaz origen del túnel, es decir, la Vlan19**. Se configuran los parámetros hello y retransmit retries para que se detecte lo más pronto posible la caída del túnel L2TP.El comando hidden permite que cualquier información sensible viaje cifrada dentro de los paquetes de control L2TP durante el establecimiento del túnel.

5.5 Tunel 1 GRE principal contra el POI NMAMNOR3

```
interface Tunnel1
 description "Tunel contra NMAMNOR3"
 ip address 10.21.34.34 255.255.255.252
 ip mtu 1476
 ip tcp adjust-mss 1436
 tunnel source 10.148.18.193
 tunnel destination 172.19.136.61
!
```

No se utiliza la facilidad de Keepalive asociada a los túneles GRE porque el POI NMAMNOR3 del fabricante Juniper no soporta dicha funcionalidad. **Debido a la fragmentación que el paquete sufre en la red de móviles, se fija la MTU del interfaz de túnel a 1476 y el tamaño de MSS (maximum segment size) se fija a 1436**. La MTU fijada viene de restar a 1500 el valor del la cabecera GRE (24 bytes).

5.6 Tunel 2 GRE backup contra el POI NMABLLA3

```
interface Tunnel2
 description "Tunel contra NMABLLA3(bck)"
 ip address 10.21.34.50 255.255.255.252
 ip mtu 1476
 ip tcp adjust-mss 1436
 tunnel source 10.148.18.193
 tunnel destination 172.19.136.129
!
```

5.7 Configuracion Routing dinamico BGP

Definición de los route-maps utilizados en la configuración de las sesiones BGP.

```
route-map Tunel_Pral_out permit 10
 set metric 150
!
route-map Tunel_Bck_in permit 10
 set local-preference 100
!
route-map Tunel_Bck_out permit 10
 set metric 200
!
route-map Tunel_Pral_in permit 10
 set local-preference 150
!
```

Definición de las sesiones BGP a través de los interfaces de túnel GRE.

```
router bgp 65000
 neighbor 10.21.34.33 remote-as 3352
 neighbor 10.21.34.49 remote-as 3352
 !
 address-family ipv4
  network 10.22.200.0 mask 255.255.255.0
  neighbor 10.21.34.33 activate
  neighbor 10.21.34.33 next-hop-self
  neighbor 10.21.34.33 route-map Tunel_Pral_in in
  neighbor 10.21.34.33 route-map Tunel_Pral_out out
  neighbor 10.21.34.49 activate
  neighbor 10.21.34.49 next-hop-self
  neighbor 10.21.34.49 route-map Tunel_Bck_in in
  neighbor 10.21.34.49 route-map Tunel_Bck_out out
```

```
 exit-address-family
!
```

Como sobre el router 887 se han definido dos interfaces lógicos de túnel, (Tunel1 y Tunel2). Sobre las IPs WAN de los túneles se definirán 2 sesiones BGP:

1. **Una sesión eBGP a través del interfaz de túnel1 principal, aquel que se establece contra el POI NMAMNOR3 designado como principal**. **Sobre dicha sesión se marcarán con métrica 150 la red LAN de la oficina móvil (10.22.200.0/24) a dicho POI** a través de las sesiones BGP que se establecen. Del mismo modo, se marcarán las redes recibidas por dicha sesión con el parámetro de bgp a Local Preference 150.
2. **Una segunda sesión eBGP a través del interfaz de túnel 2 de backup, aquel que se establece contra el POI NMABLLA3 designado como backup. Sobre dicha sesión se marcarán con métrica 200 la red LAN de la oficina móvil (10.22.200.0/24) a dicho POI a través de las sesiones BGP que se establecen**. Del mismo modo, se marcarán las redes recibidas por dicha sesión con el parámetro de bgp a Local Preference 100. Todas las redes que se quieran anunciar desde la oficina hacia la WAN se incluirán como:

```
router bgp 65000
!
 address-family ipv4
  network <red> mask <mascara>
  exit-address-family
!
!
```

5.8 Túnel IPSEC

```
interface Loopback55
 ip address 10.95.246.200 255.255.255.255
!
! Session IKE
```

```
crypto isakmp policy 10
 encr 3des
 hash md5
 authentication pre-share
 lifetime 21600
crypto isakmp key c4s3r address 0.0.0.0 0.0.0.0
crypto isakmp keepalive 60 2
!

! Definición del tráfico que se cifra
access-list 2699 remark Loopback IpSec Centrales_Cifrado
access-list 2699 permit ip 10.22.200.0 0.0.0.255 10.7.43.0 0.255.255.255
```

Se define una interfaz loopback virtual (55) que será la que se tome como origen para definir los peer que participaran en la creación del túnel IPSEC. A continuación se definen los parámetros de la sesión IKE con las siguientes características:

- Algoritmo de cifrado: **3DES**
- Algoritmo de autenticación (hash): **MD5.**
- Negociación Diffie-Hellman: **Grupo 2 (1024 bits)**
- Tiempos de vida (lifetimes): **6 horas**.
- Proceso de autenticación: **Secreto compartido**
- Keepalive: Cada **60 segundos** y perdida de **2 consecutivas**
- Clave: **Secreto Compartido**

En el equipo router central se establecerá el túnel con las mismas características. **La lista de acceso 2699 sirve para clasificar el tráfico que se cifra entre el router de la oficina móvil y el router central** La definición del origen del tráfico cifrado corresponde a la red LAN de la oficina (10.22.200.0/24) y la dirección de destino del tráfico cifrado con la red que se encuentra el servidor de monitorización en la sede central (10.7.43.0/24).

Posteriormente se define la sesión IPSEC con los siguientes parámetros:

- Algoritmo de cifrado: **esp-3des** combinado con **esp-sha-hmac**
- Tiempos de vida (lifetimes):**5horas**
- Modo de operación: **Modo Túnel.**

```
crypto ipsec security-association lifetime seconds 18000
crypto ipsec security-association replay disable
!
crypto ipsec transform-set transformada esp-3des esp-sha-hmac
crypto ipsec df-bit clear
!
crypto map mapacifrado local-address Loopback55
crypto map mapacifrado 2699 ipsec-isakmp
 set peer 10.95.246.2
 set security-association idle-time 120
 set transform-set transformada
 match address 2699
!
Interface Tunnel1
 crypto map mapacifrado
¡
Interface Tunnel2
 crypto map mapacifrado
¡
```

Se indica que la interfaz sobre la que se monta el túnel es la loopback55, y que el router remoto contra quien se quiere montar el túnel es la IP 10.95.246.2 que corresponde al interfaz loopback55 del router central de Madrid. Se indica que el tráfico que se cifra corresponde a la lista de acceso 2699 y que el tiempo de liberación del

túnel en caso de inactividad es de 120 segundos. **Se aplica el cifrado en los interfaces túneles GRE.**

5.9 Configuración SNMP para la monitorización tráfico

```
interface Loopback700
 description Loopback para monitorización SNMP
 ip address 172.29.29.200 255.255.255.255
!
router bgp 65000
address-family ipv4
      network 172.29.29.200 mask 255.255.255.255
 exit-address-family
snmp-server community caser_gestion
```

Para que el servidor de monitorización pueda atacar a un interfaz de la oficina móvil, se definirá un interfaz virtual 700 y sobre dicho interfaz se realizaran las consultas de SNMP al OID correspondiente. Adicionalmente será necesario que la IP 172.29.29.200 se anuncie a la WAN para que sea alcanzable por el servidor de monitorización.

5.10 Configuración interfaz LAN de conexión con el portátil de pruebas

```
interface FastEthernet0
 description Conexion LAN
 switchport mode access
 switchport access vlan 20
 no ip address
!
interface Vlan20
 description Vlan DATOS
```

```
 ip address 10.22.200.1 255.255.255.0
!
router bgp 65000
!
 address-family ipv4
  network 10.22.200.0 mask 255.255.255.0
exit-address-family
```

En el puerto Fa0 se asignara la vlan 20 que será la que se utilice para definir el direccionamiento LAN de la oficina. Para el portátil, la puerta de enlace será la interfaz vlan 20 y dicha red será anuncia por la WAN para que se exporte en la RPV de Caser y el servidor de monitorización tenga conectividad con el.

5.11 Configuración completa del router 887 oficina móvil

La configuración completa del router cisco 887 de la oficina móvil una vez se han realizado los pasos anteriores seria la siguiente:

```
version 15.1
service nagle
no service pad
service password-encryption
!
hostname Oficina_Movil
!
boot-start-marker
boot-end-marker
!
!
logging buffered 100000
```

```
no logging console
enable secret 4 l4RzWwqT976AnRk7OXbqX/oOWB336Lw.BoZW4NJfSpY
!
no ip source-route
!
ip dhcp pool ethant
 host 10.100.100.2 255.255.255.252
 client-identifier 7465.6c64.6174
 next-server 10.100.100.1
 option 43 ascii antenna&routertype=generic&pin=&apn=acc-caja-
1726.movistar.es&rxtimeout=360&regdenied=1"
 default-router 10.100.100.1
!
ip cef
no ip bootp server
no ip domain lookup
no ipv6 cef
l2tp-class l2tpclass1
 hidden
 hello 10
 retransmit retries 5
!
vpdn enable
!
license udi pid CISCO887VA-M-K9 sn FCZ164590HK
license accept end user agreement
license boot module c880-data level advipservices
!
controller VDSL 0
```

```
!
pseudowire-class pwclass1
 encapsulation l2tpv2
 protocol l2tpv2 l2tpclass1
 ip local interface Vlan19
!
crypto isakmp policy 10
 encr 3des
 hash md5
 authentication pre-share
 lifetime 21600
crypto isakmp key c4s3r address 0.0.0.0 0.0.0.0
crypto isakmp keepalive 60
!
crypto ipsec security-association lifetime seconds 18000
crypto ipsec security-association replay disable
!
crypto ipsec transform-set transformada esp-3des esp-sha-hmac
crypto ipsec df-bit clear
!
crypto map mapacifrado local-address Loopback55
crypto map mapacifrado 2699 ipsec-isakmp
 set peer 10.95.246.2
 set security-association idle-time 120
 set transform-set transformada
 match address 2699
!
!
interface Loopback55
```

```
 ip address 10.95.246.200 255.255.255.255
!
interface Loopback700
 ip address 172.29.29.200 255.255.255.255
!
interface Tunnel1
 description "Tunel contra NMAMNOR3"
 ip address 10.21.34.34 255.255.255.252
 ip mtu 1476
 ip tcp adjust-mss 1436
 tunnel source 10.148.18.193
 tunnel destination 172.19.136.61
 crypto map mapacifrado
!
interface Tunnel2
 description "Tunel contra NMABLLA3(bck)"
 ip address 10.21.34.50 255.255.255.252
 ip mtu 1476
 ip tcp adjust-mss 1436
 tunnel source 10.148.18.193
 tunnel destination 172.19.136.129
 crypto map mapacifrado
!
interface Ethernet0
 no ip address
 shutdown
!
interface ATM0
 no ip address
```

```
 shutdown
 no atm ilmi-keepalive
!
interface FastEthernet0
 description Conexion LAN
 switchport access vlan 20
 no ip address
 load-interval 30
 no cdp enable
!
interface FastEthernet1
shutdown
!
interface FastEthernet2
shutdown
!
interface FastEthernet3
 description Conexion Antena Ethernet UMTS
 switchport access vlan 19
 no ip address
!
interface Virtual-PPP1
 ip address negotiated
 ppp pfc local request
 ppp pfc remote apply
 ppp acfc local request
 ppp acfc remote apply
 ppp chap hostname 1726_sucursal156@vpn-mv-acc-caja-1726
 ppp chap password caja1726
```

```
 no cdp enable
 pseudowire 10.100.100.2 1 pw-class pwclass1
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan19
 description Vlan Conexion ANTENA_UMTS
 ip address 10.100.100.1 255.255.255.252
!
interface Vlan20
 description Vlan DATOS
 ip address 10.22.200.1 255.255.255.0
!
router bgp 65000
 bgp log-neighbor-changes
 neighbor 10.21.34.33 remote-as 3352
 neighbor 10.21.34.49 remote-as 3352
 !
 address-family ipv4
  network 10.22.200.0 mask 255.255.255.0
  network 10.95.246.200 mask 255.255.255.255
  network 172.29.29.200 mask 255.255.255.255
  neighbor 10.21.34.33 activate
  neighbor 10.21.34.33 next-hop-self
  neighbor 10.21.34.33 route-map Tunel_Pral_in in
  neighbor 10.21.34.33 route-map Tunel_Pral_out out
  neighbor 10.21.34.49 activate
```

```
  neighbor 10.21.34.49 next-hop-self
  neighbor 10.21.34.49 route-map Tunel_Bck_in in
  neighbor 10.21.34.49 route-map Tunel_Bck_out out
 exit-address-family
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
ip route profile
ip route 172.19.136.61 255.255.255.255 Virtual-PPP1
ip route 172.19.136.129 255.255.255.255 Virtual-PPP1
!
access-list 2699 remark Loopback IpSec Centrales_Cifrado
access-list 2699 permit ip 10.22.200.0 0.0.0.255 10.7.43.0 0.255.255.255
snmp-server community caser_gestion
no cdp run
!
!
route-map Tunel_Pral_out permit 10
 set metric 150
!
route-map Tunel_Bck_in permit 10
 set local-preference 100
!
route-map Tunel_Bck_out permit 10
 set metric 200
!
route-map Tunel_Pral_in permit 10
```

```
 set local-preference 150
!
line con 0
 exec-timeout 5 0
 no modem enable
line aux 0
 modem InOut
 no exec
 stopbits 1
 flowcontrol hardware
line vty 0 4
 exec-timeout 30 0
 password 7 06155F601C4D590B00
 transport input all
```

6 CONFIGURACION ROUTER OFICINA CENTRAL

Para el router de la oficina central, **la configuración a realizar para que la oficina móvil tenga conectividad con el servidor de monitorización será necesario anunciar la red 10.11.43.0/24 hacia la WAN mediante el protocolo de routing dinámico correspondiente, en este caso mediante RIPv2.** La red **10.95.246.2 también será necesario anunciarla para montar el túnel IPSEC** y por ultimo realizar la configuración del túnel IPSEC en este extremo. Por lo general, en el este router central se configurara un túnel por cada oficina de Caser que pertenece a su RPV. En este caso solo pondré la parte de configuración necesaria del túnel para montarlo con la oficina móvil.

6.1 Configuración túnel IPSEC

```
interface Loopback55
 ip address 10.95.246.2 255.255.255.255
!
!Sesion IKE
```

```
crypto isakmp policy 10
 encr 3des
 hash md5
 authentication pre-share
 lifetime 21600
crypto isakmp key c4s3r address 0.0.0.0
crypto isakmp keepalive 60 2
!
!Definicion trafico que se cifra
access-list 2100 remark Tunel IPSEC contra Oficina Movil
access-list 2100 permit ip 10.7.43.0 0.0.0.255 10.22.200.0 0.0.0.255
!Sesion IPSEC
crypto ipsec security-association lifetime seconds 18000
crypto ipsec security-association replay disable
!
crypto ipsec transform-set transformada esp-3des esp-sha-hmac
 mode tunnel
crypto ipsec df-bit clear
!
crypto map mapacifrado 2100 ipsec-isakmp
 set peer 10.95.246.200
 set security-association idle-time 120
 set transform-set transformada
 match address 2100
```

6.2 Configuración routing dinámico

```
router rip
 version 2
 redistribute connected
```

```
 redistribute static
 network 172.18.0.0
 network 172.19.0.0
 network 10.95.246.2
 no auto-summary
!
ip route 10.11.43.0 255.255.255.0 172.26.204.1
```

Esta es la parte de configuración del routing de RIP para anunciar la red de loopback55 del túnel y la red 10.11.43.0/24 del servidor de monitorización. Se pone una ruta estática y se redistribuye por RIP ya que la red donde esta el servidor no esta directamente conectada al router central y tiene que ser alcanzada a través de un router Gateway (172.26.204.1) de Caser.

7 PILA DE PROTOCOLOS QUE INTERVIENEN EN LA SOLUCIÓN

El proceso de protocolos que intervienen en el funcionamiento de la oficina móvil para el portátil de pruebas (10.22.200.2) tenga conectividad con el servidor de monitorización (10.11.43.29) es el siguiente:

1- El router **cisco 887 por DHCP le pasa a la antena 3G el direccionamiento IP y los parámetros de acceso 3G** y de control.

2- **Establecer un túnel L2TP pseudowaire entre el interfaz vlan 19 del router 887 y la antena 3G para el transporte del protocolo PPP**.

3- **El router efectúa una llamada a través de la interfaz radio de la antena al Punto de Acceso (APN) designado para Caser (acc-caja-1726.movistar.es)**. La llamada es recibida por el equipo de la red SGSN. Dicho equipo consulta la base de datos de abonados HLR para verificar si el número llamante que originó la llamada esta subscrito al APN solicitado.

4- **El SGSN que ha registrado la llamada progresa la conexión hasta el GGSN correspondiente.** En concreto el SGSN que registra la llamada establece un túnel GPRS (GTP: GPRS Tunneling Protocol) contra el GGSN que actúa como pasarela.

5- **El GGSN que recibe la conexión negocia el establecimiento de una conexión Punto a Punto (PPP)** con el router 887 de la oficina móvil.

5.1 - En la primera **parte de la negociación PPP: LCP** (Link Control Protocol), se determina básicamente el tamaño de trama (MRU: Maximum Reception Unit) y el protocolo a través del cual el router va a intercambiar las claves de acceso mediante CHAP.

5.2- Tras efectuarse la negociación inicial el equipo **GGSN consulta al servidor Radius Conserv11 para validar los datos de usuario/password** indicados por el router.

5.3- **El radius Conserv11 consulta a la Base de Datos LDAP nmamsep3 el usuario y password estén en dicha BBDD.** Adicionalmente **en la consulta se obtiene la IP que deberá ser asignada a la interfaz virtual-ppp1 WAN del router 887, en nuestro caso la IP 10.148.18.193** que coincide con la IP túnel origen de GRE.

5.4-Una vez validado el acceso se inicia la segunda parte de la negociación PPP (IPCP: IP Control Protocol), donde se determinan los parámetros del nivel de red asociados a la conexión. En concreto en nuestro **caso el GGSN le indica al router la dirección IP WAN que debe emplear para el interfaz virtual-ppp1** que se comento en el punto 5.3.

6- Una vez asignada la IP WAN al interfaz virtual-**ppp1 se montaran los túneles GRE contra los POI de la red IP Única** que encapsulara el trafico IP que se genera desde el router.

7- Para dar visibilidad de las redes que tienen en la oficina móvil en la RPV de Caser (vpn_34A28013050_172600) **se establece vecindad de rountig BGP a través de los túneles GRE con los POIs para que ambos equipos intercambien las tablas de rutas** de las redes que se conocen a traves de la RPV.

8- Por ultimo una **vez que se conozcan las redes de la oficina móvil y se genere trafico contra el servidor de monitorización, se montara el túnel IPSEC, primero la sesión IKE de negociado, autenticación y cifrado de claves y posteriormente la fase dos del protocolo IPSEC para cifrar el paquete IP.**

En la siguiente figura se muestra un esquema de los protocolos y pasos anteriormente comentados.

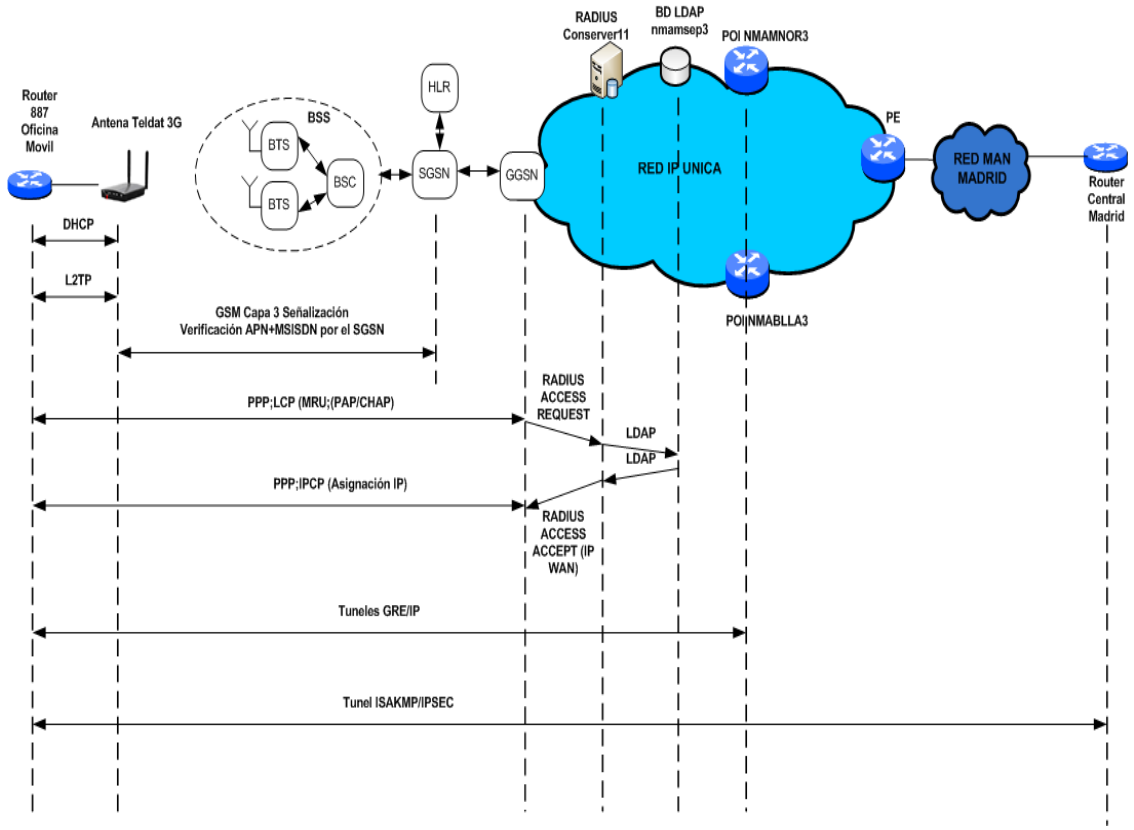


Figura 8.7.1 Esquema de red que intervienen en la práctica de la oficina móvil. Elaboración propia

8 TROUBLESHOOTING PARA COMPROBAR EL FUNCIONAMIENTO

8.1 Comprobar la conectividad del portátil con el router

Para comprobar la conectividad del portátil de pruebas con el router 887, primero tenemos que configurar en los parámetros del red del portátil la IP 10.22.200.2 con mascara 255.255.255.0 y su puerta de enlace la 10.22.200.2. **Una vez realizado este trabajo lanzamos un ping contra la puerta de enlace para verificar que el direccionamiento y el cableado UTP están correctamente enchufados al router.**

```
D:\Users\Administrador>ping 10.22.200.1

Haciendo ping a 10.22.200.1  con 32 bytes de datos:
Respuesta desde 10.22.200.1 : bytes=32 tiempo=1ms TTL=63
Respuesta desde 10.22.200.1 : bytes=32 tiempo<1m TTL=63
Respuesta desde 10.22.200.1 : bytes=32 tiempo<1m TTL=63
Respuesta desde 10.22.200.1 : bytes=32 tiempo<1m TTL=63

Estadísticas de ping para 10.22.200.1:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 1ms, Media = 0ms
```

Figura 8.8.1 Captura de trafico icmp lanzado desde el portátil de pruebas a la puerta de enlace para comprobar la conectividad.

En la **tabla de rutas del PC vemos que para alcanzar cualquier red, eso incluye la del servidor de monitorización (10.11.43.0/24)** en siguiente **salto es la IP 10.22.200.1** que corresponde a la IP de la vlan 20 del router 887.

```
Rutas activas:
Destino de red         Máscara de red   Puerta de enlace   Interfaz  Métrica
          0.0.0.0         0.0.0.0      10.22.200.1      10.22.200.2     276
      10.22.200.0   255.255.255.0      En vínculo       10.22.200.2     276
      10.22.200.2   255.255.255.255    En vínculo       10.22.200.2     276
    10.22.200.255   255.255.255.255    En vínculo       10.22.200.2     276
        127.0.0.0         255.0.0.0    En vínculo         127.0.0.1     306
        127.0.0.1   255.255.255.255    En vínculo         127.0.0.1     306
  127.255.255.255   255.255.255.255    En vínculo         127.0.0.1     306
        224.0.0.0         240.0.0.0    En vínculo         127.0.0.1     306
        224.0.0.0         240.0.0.0    En vínculo       10.22.200.2     276
  255.255.255.255   255.255.255.255    En vínculo         127.0.0.1     306
  255.255.255.255   255.255.255.255    En vínculo       10.22.200.2     276
===========================================================================
Rutas persistentes:
  Dirección de red  Máscara de red  Dirección de puerta de enlace  Métrica
          0.0.0.0         0.0.0.0      10.22.200.1  Predeterminada
===========================================================================
```

Figura 8.8.2 Captura de la tabla de rutas del portátil de pruebas.

8.2 Verificar el funcionamiento de DHCP del router con la antena 3G

Desde el router Cisco 887 con los mandatos **show ip dhcp Server statistics y show ip dhcp binding podemos ver los mensajes de DHCP intercambiados entre el router y la antena** y la IP que se le ha asignado a la antena asi como el tiempo de uso de dicha IP, que en este caso es infinito.

```
Oficina_Movil#show ip dhcp server statistics
Memory usage         23885
```

Address pools 1
Database agents 0
Automatic bindings 0
Manual bindings 1
Expired bindings 0
Malformed messages 0
Secure arp entries 0

Message Received
BOOTREQUEST 0
DHCPDISCOVER 294
DHCPREQUEST 94
DHCPDECLINE 0
DHCPRELEASE 0
DHCPINFORM 39875

Message Sent
BOOTREPLY 0
DHCPOFFER 38
DHCPACK 39969
DHCPNAK 0

Oficina_Movil#sh ip dhcp binding
Bindings from all pools not associated with VRF:
IP address Client-ID/ Lease expiration Type
Hardware address/
User name
10.100.100.2 7465.6c64.6174 **Infinite** Manual

Una vez que vemos que se le ha asignado la IP **10.100.100.2 a la antena podemos acceder a ella mediante Telnet desde el router y verificar que los parámetros de**

configuración de acceso a la red 3G (APN entre otros son correctos) mediante el comando showmonitor que le pasa el router por DHCP mediante la opcion 43.

```
Oficina_Movil#sh arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  10.22.200.1            -   6073.5cc7.e45a  ARPA   Vlan20
Internet  10.100.100.1           -   6073.5cc7.e45a  ARPA   Vlan19
Internet  10.100.100.2           0   00a0.2622.320a  ARPA   Vlan19
```

```
Oficina_Movil#telnet 10.100.100.2
Trying 10.100.100.2 ... Open
01.27-EthAnt-00 login: monitor
Password: teldat

Welcome to the Teldat 3Ge equipment. Teldat 2008.
------------------------------------------------------------------------
?                    help                 allhelp
------------------------------------------------------------------------
exit                 l2tp-restart         pppoe-restart
restart
------------------------------------------------------------------------
downloadapp          showupdate           uptimehours
------------------------------------------------------------------------
hide                 l2tp-debug-level     pppoe-debug-level
view                 bitrate              showcoverage
showmonitor          showdebug
------------------------------------------------------------------------
clearlog             showlog
------------------------------------------------------------------------
changepw             restoreconfig        setdefaultconfig
showconfig           timeset
------------------------------------------------------------------------
```

atattach atcall atcommand

atdetach athangup atinitialcfg

wwanmanufacturer atgsm atdgsm

atreset puk pinchange

wwanupgrade

Enter a command>**showmonitor**

Running version: Oct 25 14:15:00 2011#01.27-EthAnt-00

Flash version: Oct 25 14:15:00 2011#01.27-EthAnt-00

Power supply: POE

Power supply on reset: POE

eth0: **status: link up**, 100MBit Full Duplex, auto-negotiation complete.

MAC 00:A0:26:22:32:0A

localip 10.100.100.2

netmask 255.255.255.252

tftpserver 10.100.100.1

boot_file fwethant.img

gateway 10.100.100.1

object_vsi **antenna&routertype=generic&pin=****=acc-caja-1726.movistar.es&rxtimeout=360&regdenied=1** **<- Parametros acceso red 3G**

RX

packets:2359

errors:0

dropped:0

overruns:0

frame:0

TX

packets:1684

errors:0

dropped:0

overruns:0

8.3 Tunel L2TP entre router 887 y antena 3G

Para **verificar que se ha establecido el tunel L2TP** entre la interfaz vlan 19 de router 887 (10.100.100.1) con la antena 3G (10.100.100.2) metemos el **mandato show l2tp tunnel y nos indicara datos de la sesion L2TP establecida:**

Oficina_Movil#show l2tp tunnel

L2TP Tunnel Information Total tunnels 1 sessions 1

LocTunID	RemTunID	Remote Name	State	Remote Address	Sessn Count	L2TP Class/ VPDN Group
32129	12757	01.27-EthAnt-	**est**	**10.100.100.2**	1	l2tpclass1

Introduciendo el mandato **debug l2tp packet event en el router cisco podremos ver las trazas para ver como se ha establecido el tunel L2TP entre el y la antena**. Estas son las trazas que se obtuvieron:

Apr 15 11:41:24.359 METDST: L2TP tnl 10029:0000652A: O SCCRQ to **10.100.100.2**
Apr 15 11:41:24.359 METDST: L2TP tnl 10029:0000652A: IETF v2:
Apr 15 11:41:24.359 METDST: L2TP tnl 10029:0000652A: Protocol Version 1, Revision 0
Apr 15 11:41:24.359 METDST: L2TP tnl 10029:0000652A: Framing Cap none(0x0)
Apr 15 11:41:24.359 METDST: L2TP tnl 10029:0000652A: Tie Breaker
Apr 15 11:41:24.359 METDST: L2TP tnl 10029:0000652A: D2FCB861658EB3C3
Apr 15 11:41:24.359 METDST: L2TP tnl 10029:0000652A: Firmware Ver 0x1130
Apr 15 11:41:24.359 METDST: L2TP tnl 10029:0000652A: Hostname **"Oficina_Movil"**
Apr 15 11:41:24.359 METDST: L2TP tnl 10029:0000652A: Vendor Name
Apr 15 11:41:24.359 METDST: L2TP tnl 10029:0000652A: "Cisco Systems, Inc."
Apr 15 11:41:24.359 METDST: L2TP tnl 10029:0000652A: Assigned Tunnel I 0x0000652A (25898)
Apr 15 11:41:24.359 METDST: L2TP tnl 10029:0000652A: Rx Window Size 512
Apr 15 11:41:24.359 METDST: L2TP tnl 10029:0000652A: PPPoE Relay Response Capable
Apr 15 11:41:24.359 METDST: L2TP tnl 10029:0000652A: PPPoE Relay Forward Capable
Apr 15 11:41:24.363 METDST: L2TP tnl 10029:0000652A: Cisco v2:
Apr 15 11:41:24.363 METDST: L2TP tnl 10029:0000652A: PPPoE Relay Forward Capable

Apr 15 11:41:24.363 METDST: L2TP tnl 10029:0000652A: PPPoE Relay Response Capable
Apr 15 11:41:24.363 METDST: L2TP tnl 10029:0000652A:
Apr 15 11:41:27.375 METDST: L2TP tnl 10029:0000652A: Drain unsentQ, cur/max resendQ sz 0/4, unsentQ 0
Apr 15 11:41:27.375 METDST: L2TP tnl 10029:0000652A:
Apr 15 11:41:27.375 METDST: L2TP tnl 10029:0000652A: I SCCRP, flg TLS, ver 2, len 92
Apr 15 11:41:27.375 METDST: L2TP tnl 10029:0000652A: IETF v2:
Apr 15 11:41:27.375 METDST: L2TP tnl 10029:0000652A: Protocol Version 1, Revision 0
Apr 15 11:41:27.375 METDST: L2TP tnl 10029:0000652A: Framing Cap both(0x3)
Apr 15 11:41:27.375 METDST: L2TP tnl 10029:0000652A: Hostname **"01.27-EthAnt-00"**
Apr 15 11:41:27.375 METDST: L2TP tnl 10029:0000652A: Vendor Name
Apr 15 11:41:27.375 METDST: L2TP tnl 10029:0000652A: "Teldat S.A."
Apr 15 11:41:27.375 METDST: L2TP tnl 10029:0000652A: Assigned Tunnel I 0x0000B2C1 (45761)
Apr 15 11:41:27.375 METDST: L2TP tnl 10029:0000652A: Rx Window Size 4
Apr 15 11:41:27.375 METDST: L2TP tnl 10029:0000652A:
Apr 15 11:41:27.375 METDST: L2TP tnl 10029:0000652A: I SCCRP from 01.27-EthAnt-00
Apr 15 11:41:27.375 METDST: L2TP tnl 10029:0000652A:
Apr 15 11:41:27.375 METDST: L2TP tnl 10029:0000652A: O SCCCN to 01.27-EthAnt-00 tnl 45761
Apr 15 11:41:27.379 METDST: L2TP tnl 10029:0000652A:
Apr 15 11:41:27.379 METDST: L2TP 00001:10029:0000714E: O ICRQ to 01.27-EthAnt-00 45761/0
Apr 15 11:41:27.379 METDST: L2TP 00001:10029:0000714E: IETF v2:
Apr 15 11:41:27.379 METDST: L2TP 00001:10029:0000714E: Assigned Call ID 0x0000714E (29006)
Apr 15 11:41:27.379 METDST: L2TP 00001:10029:0000714E: Serial Number 2433900012
Apr 15 11:41:27.379 METDST: L2TP 00001:10029:0000714E:
Apr 15 11:41:27.383 METDST: L2TP tnl 10029:0000652A: Drain unsentQ, cur/max resendQ sz 0/4, unsentQ 0
Apr 15 11:41:27.383 METDST: L2TP tnl 10029:0000652A:
Apr 15 11:41:27.383 METDST: L2TP 00001:10029:0000714E: I ICRP, flg TLS, ver 2, len 28
Apr 15 11:41:27.383 METDST: L2TP 00001:10029:0000714E: IETF v2:
Apr 15 11:41:27.383 METDST: L2TP 00001:10029:0000714E: Assigned Call ID 0x00008B16 (35606)
Apr 15 11:41:27.387 METDST: L2TP 00001:10029:0000714E:

Apr 15 11:41:27.387 METDST: L2TP 00001:10029:0000714E: O ZLB ACK to 01.27-EthAnt-00 45761/35606
Apr 15 11:41:27.387 METDST: L2TP 00001:10029:0000714E:
Apr 15 11:41:27.391 METDST: L2TP 00001:10029:0000714E: O ICCN to 01.27-EthAnt-00 45761/35606
Apr 15 11:41:27.391 METDST: L2TP 00001:10029:0000714E: IETF v2:
Apr 15 11:41:27.391 METDST: L2TP 00001:10029:0000714E: Framing Type none(0)
Apr 15 11:41:27.391 METDST: L2TP 00001:10029:0000714E: Connect Speed 0
Apr 15 11:41:27.391 METDST: L2TP 00001:10029:0000714E:
Apr 15 11:41:30.971 METDST: L2TP tnl 10029:0000652A: Drain unsentQ, cur/max resendQ sz 0/4, unsentQ 0
Apr 15 11:41:30.971 METDST: L2TP tnl 10029:0000652A:
Apr 15 11:41:30.971 METDST: L2TP tnl 10029:0000652A: I ZLB ACK, flg TLS, ver 2, len 12
Apr 15 11:41:30.971 METDST: L2TP tnl 10029:0000652A:
Apr 15 11:41:30.999 METDST: L2TP tnl 10029:0000652A: I ZLB ACK, flg TLS, ver 2, len 12
Apr 15 11:41:30.999 METDST: L2TP tnl 10029:0000652A:

Una vez establecido **el túnel tal y como se muestra en las anteriores trazas el interfaz virtual-ppp1 pasara a levantarse para comenzar el negociado, autenticación y transporte del protocolo PPP de nivel 2** contra el equipo GGSN de la red móvil.

Apr 15 11:41:31.067 METDST: %LINEPROTO-5-UPDOWN: **Line protocol on Interface Virtual-PPP1, changed state to up**

8.4 Parámetros de cobertura de la antena 3G

Una vez que el router efectúa la llamada contra la estación base y queda registrado en el APN correspondiente, se puede verificar los parámetros de cobertura obtenidos. **Para comprobar los parámetros de cobertura de la antena 3G y bajo que tecnología esta funcionando (GPRS,UMTS,HSDPA…) se puede hacer desde dos vías**:

1- **Accediendo por Telnet a la IP de la antena y con el mandato showcoverage** comprobar los parámetros de cobertura.

2- **La segunda opción es por http** poniendo en el portátil de pruebas en un navegador la IP de la antena. Esta opción es más recomendable ya que presenta un interfaz más amigable y de fácil lectura.

Al emplear la segunda opción es necesario verificar antes que desde el portátil de pruebas se tiene conectividad IP con la antena 3G. Para ello lanzamos un ping:

```
D:\Users\Administrador>ping 10.100.100.2

Haciendo ping a 10.100.100.2 con 32 bytes de datos:
Respuesta desde 10.100.100.2: bytes=32 tiempo=1ms TTL=63
Respuesta desde 10.100.100.2: bytes=32 tiempo<1m TTL=63
Respuesta desde 10.100.100.2: bytes=32 tiempo<1m TTL=63
Respuesta desde 10.100.100.2: bytes=32 tiempo<1m TTL=63

Estadísticas de ping para 10.100.100.2:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 1ms, Media = 0ms
```

Figura 8.8.3 Captura de trafico ICMP lanzado desde el portátil de pruebas a la IP LAN de la antena Teldat.

Con un traceroute vemos que el primer salto es el interfaz del router 887 correspondiente a la vlan 20 y el siguiente salto es la IP de la antena que pertenece a la red 10.100.100.0/30

```
D:\Users\Administrador>tracert 10.100.100.2

Traza a 10.100.100.2 sobre caminos de 30 saltos como máximo.

  1    <1 ms    <1 ms    <1 ms  10.22.200.1
  2    <1 ms    <1 ms    <1 ms  10.100.100.2

Traza completa.
```

Figura 8.8.4 Captura de un traceroute lanzado desde el portátil de pruebas a la IP LAN de la antena Teldat para observar el camino que recorre.

Una vez verificada la conectividad IP con la antena, **nos abrimos un navegador web y en la url metemos la IP 10.100.100.2**. Nos salta una ventana pidiéndonos un usuario (monitor) y password (teldat)

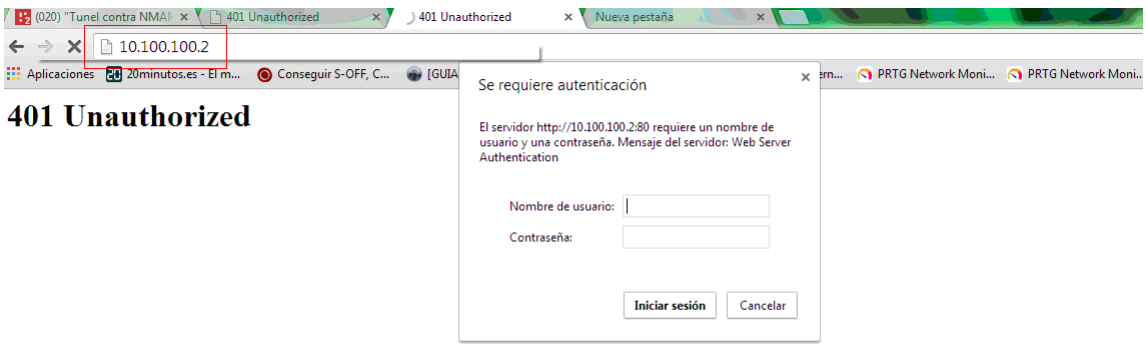


Figura 8.8.5 Captura de la página web que aperece al acceder por http a la antena Teldat para que se introduzca usuario y password.

Una vez que nos autenticamos nos aparecerá la siguiente ventana con un menú en el que podemos elegir diferentes opciones:

Figura 8.8.6 Captura de la página web del menu de parámetros observables por http en la antena Teldat.

Dentro del menú seleccionamos la opción WWAN y nos mostrara la siguiente ventana:

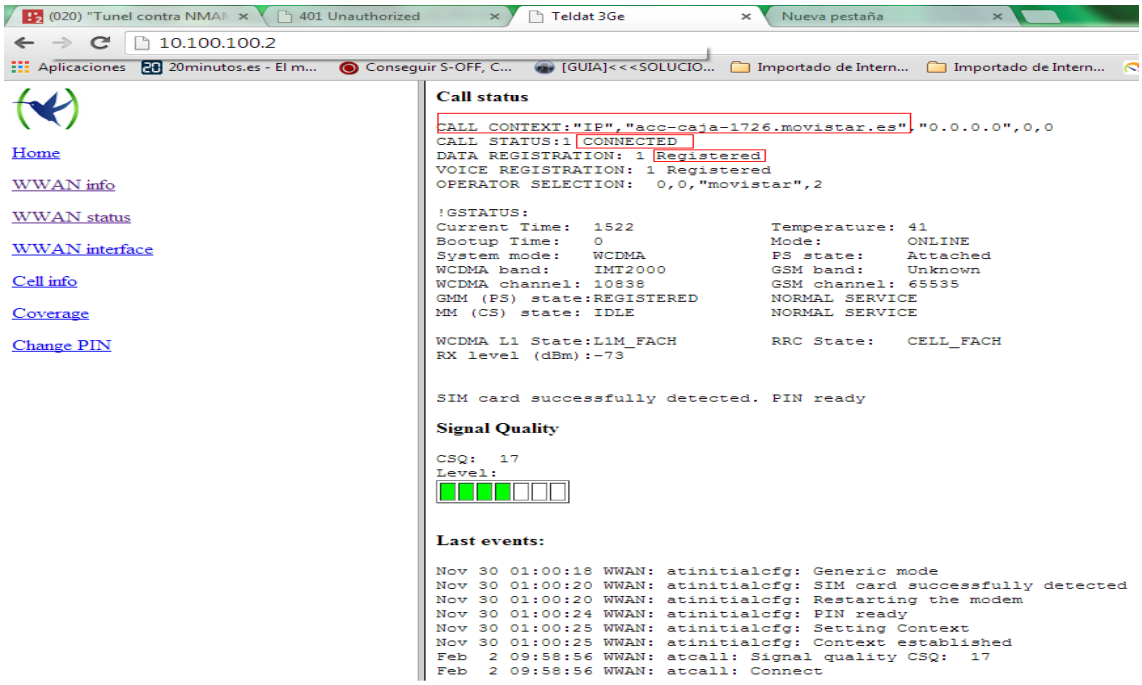


Figura 8.8.7 Captura de la página web donde se observan el APN, el estado de la red y si esta registrada la antena Teldat.

En la ventana anterior podemos ver el APN que se encuentra registrada la SIM, que esta en estado conectado y una serie de parámetros adicionales. Por ultimo si pulsamos en el menú Cell Info obtendremos la información de los parámetros de la señal recibida y con que calidad y potencia así como sobre que tecnología esta trabajando:

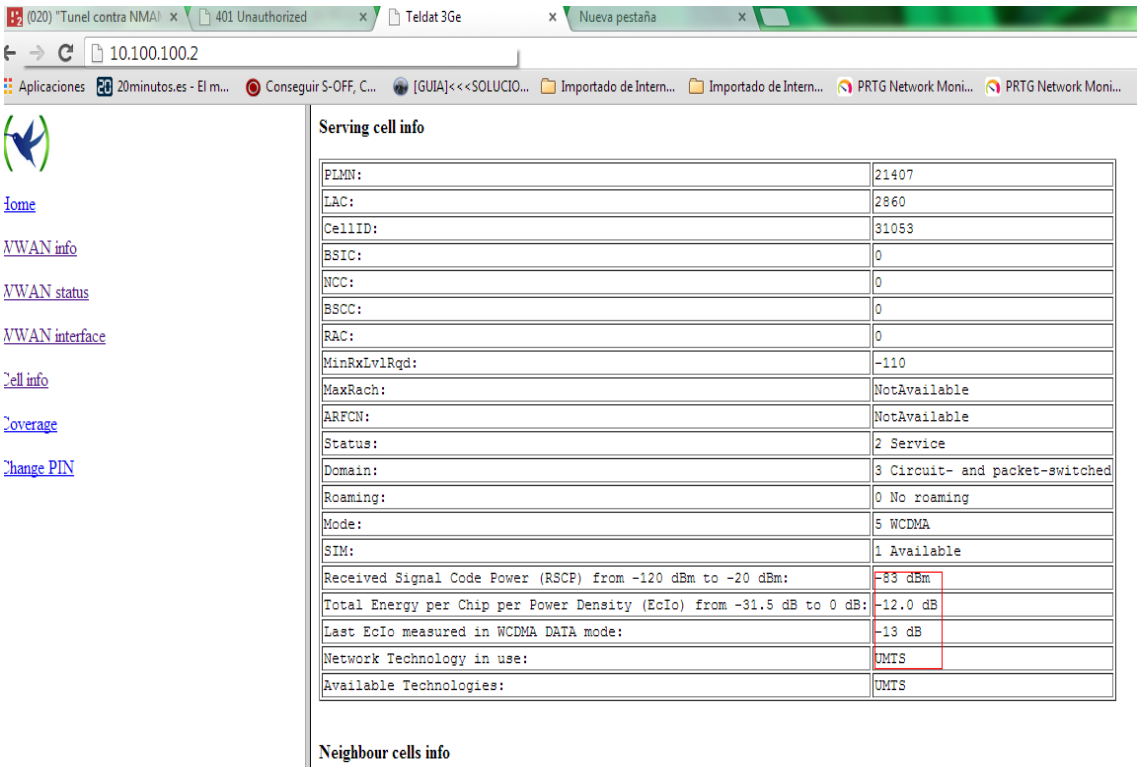


Figura 8.8.8 Captura de la página web donde los parámetros de la señal recibida, interferencias y calidad de la misma en la antena Teldat.

En la **captura anterior se puede apreciar que esta trabajando bajo tecnología UMTS cuyo potencia de la señal recibida (RSCP) es de -83dBm y los parámetros de calidad e interferencias (EcIo) es -12 dB.**

8.5 Establecimiento de la conexión PPP en el router

Comprobamos que el **interfaz virtual-ppp1 este levantado pero no tiene IP asignada**:

```
Oficina_Movil#sh ip inter brief
Interface              IP-Address      OK? Method  Status                Protocol
ATM0                   unassigned      YES NVRAM   administratively down down
Ethernet0              unassigned      YES NVRAM   administratively down down
```

FastEthernet0	unassigned	YES unset	down	down
FastEthernet1	unassigned	YES unset	down	down
FastEthernet2	unassigned	YES unset	down	down
FastEthernet3	unassigned	YES unset	up	up
Loopback55	10.95.246.112	YES NVRAM	up	up
Loopback600	10.222.131.220	YES NVRAM	up	up
Tunnel1	10.21.34.34	YES NVRAM	up	down
Tunnel2	10.21.34.50	YES NVRAM	up	down
Virtual-PPP1	**unassigned**	**YES IPCP**	**up**	**up**
Vlan1	unassigned	YES unset	administratively down	down
Vlan19	10.100.100.1	YES NVRAM	up	up
Vlan20	10.22.200.1	YES NVRAM	down	down

El método de **asignación de la IP en el interfaz virtual-ppp1 es IPCP lo que significa que una vez que se establece la sesión PPP con el GGSN, este consultar al radius Conserv11 para que verifique si en la BBDD de LDAP esta dado de alta**. Si esta dado de alta el radius le notificara al GGSN que IP tiene que llevar asociada dicha interfaz y el GGSN le indicara mediante el protocolo IPCP al router la IP que debe configurarse. **Para ver las trazas del establecimiento del protocolo PPP tenemos que introducir en el router los mandatos debug ppp authentication y debug ppp negociation** y nos mostrara lo siguiente:

Apr 15 11:47:23.799 METDST: Vp1 PPP: Using default call direction
Apr 15 11:47:23.799 METDST: Vp1 PPP: Treating connection as a dedicated line
Apr 15 11:47:23.799 METDST: Vp1 PPP: Session handle[4400000D] Session id[1]
Apr 15 11:47:23.799 METDST: Vp1 LCP: **Event[OPEN] State[Initial to Starting]**
Apr 15 11:47:23.799 METDST: Vp1 LCP: O CONFREQ [Starting] id 1 len 14
Apr 15 11:47:23.799 METDST: Vp1 LCP: MagicNumber 0x73D9CC13 (0x050673D9CC13)
Apr 15 11:47:23.799 METDST: Vp1 LCP: PFC (0x0702)
Apr 15 11:47:23.799 METDST: Vp1 LCP: ACFC (0x0802)
Apr 15 11:47:23.799 METDST: Vp1 LCP: Event[UP] State[Starting to REQsent]
Apr 15 11:47:25.799 METDST: Vp1 LCP: O CONFREQ [REQsent] id 2 len 14
Apr 15 11:47:25.799 METDST: Vp1 LCP: MagicNumber 0x73D9CC13 (0x050673D9CC13)
Apr 15 11:47:25.799 METDST: Vp1 LCP: PFC (0x0702)
Apr 15 11:47:25.799 METDST: Vp1 LCP: ACFC (0x0802)
Apr 15 11:47:25.799 METDST: Vp1 LCP: Event[Timeout+] State[REQsent to REQsent]
Apr 15 11:47:27.395 METDST: Vp1 PPP: I pkt type 0xC021, datagramsize 21 link[ppp]

Apr 15 11:47:27.395 METDST: Vp1 LCP: I CONFREQ [REQsent] id 15 len 19

Apr 15 11:47:27.395 METDST: Vp1 LCP: **AuthProto CHAP (0x0305C22305)**

Apr 15 11:47:27.395 METDST: Vp1 LCP: MagicNumber 0x011873FC (0x0506011873FC)

Apr 15 11:47:27.395 METDST: Vp1 LCP: PFC (0x0702)

Apr 15 11:47:27.395 METDST: Vp1 LCP: ACFC (0x0802)

Apr 15 11:47:27.395 METDST: Vp1 LCP: O CONFACK [REQsent] id 15 len 19

Apr 15 11:47:27.395 METDST: Vp1 LCP: AuthProto CHAP (0x0305C22305)

Apr 15 11:47:27.395 METDST: Vp1 LCP: MagicNumber 0x011873FC (0x0506011873FC)

Apr 15 11:47:27.395 METDST: Vp1 LCP: PFC (0x0702)

Apr 15 11:47:27.395 METDST: Vp1 LCP: ACFC (0x0802)

Apr 15 11:47:27.395 METDST: Vp1 LCP: Event[Receive ConfReq+] State[REQsent to ACKsent]

Apr 15 11:47:27.403 METDST: Vp1 PPP: I pkt type 0xC021, datagramsize 16 link[ppp]

Apr 15 11:47:27.403 METDST: Vp1 LCP: I CONFACK [ACKsent] id 2 len 14

Apr 15 11:47:27.403 METDST: Vp1 LCP: MagicNumber 0x73D9CC13 (0x050673D9CC13)

Apr 15 11:47:27.403 METDST: Vp1 LCP: PFC (0x0702)

Apr 15 11:47:27.403 METDST: Vp1 LCP: ACFC (0x0802)

Apr 15 11:47:27.403 METDST: Vp1 LCP: Event[Receive ConfAck] State[ACKsent to Open]

Apr 15 11:47:27.427 METDST: Vp1 LCP-FS: I DISCREQ [Open] id 16 len 8 magic 0x011873FC

Apr 15 11:47:27.431 METDST: Vp1 PPP: Phase is AUTHENTICATING, by the peer

Apr 15 11:47:27.431 METDST: Vp1 LCP: State is Open

Apr 15 11:47:27.431 METDST: Vp1 PPP: I pkt type 0xC223, datagramsize 37 link[ppp]

Apr 15 11:47:27.435 METDST: Vp1 CHAP: I CHALLENGE id 1 len 35 from "UMTS_CHAP_SRVR"

Apr 15 11:47:27.435 METDST: Vp1 PPP: Sent CHAP SENDAUTH Request

Apr 15 11:47:27.435 METDST: Vp1 PPP: Received SENDAUTH Response FAIL

Apr 15 11:47:27.435 METDST: Vp1 CHAP: Using hostname from interface CHAP

Apr 15 11:47:27.435 METDST: Vp1 CHAP: Using password from interface CHAP

Apr 15 11:47:27.435 METDST: Vp1 CHAP: O **RESPONSE id 1 len 58 from "1726_sucursal156@vpn-mv-acc-caja-1726"**

Apr 15 11:47:27.455 METDST: Vp1 PPP: I pkt type 0xC223, datagramsize 6 link[ppp]

Apr 15 11:47:27.455 METDST: Vp1 **CHAP: I SUCCESS id 1 len 4**

Apr 15 11:47:27.455 METDST: Vp1 **PPP: Phase is UP**

Apr 15 11:47:27.459 METDST: Vp1 IPCP: Protocol configured, start CP. state[Initial]

Apr 15 11:47:27.459 METDST: Vp1 IPCP: Event[OPEN] State[Initial to Starting]

Apr 15 11:47:27.459 METDST: Vp1 IPCP: O CONFREQ [Starting] id 1 len 10

Apr 15 11:47:27.459 METDST: Vp1 IPCP: **Address 0.0.0.0 (0x030600000000)**

Apr 15 11:47:27.459 METDST: Vp1 IPCP: Event[UP] State[Starting to REQsent]

Apr 15 11:47:28.487 METDST: Vp1 PPP: I pkt type 0x8021, datagramsize 18 link[ip]

Apr 15 11:47:28.487 METDST: Vp1 IPCP: I CONFNAK [REQsent] id 1 len 16

Apr 15 11:47:28.487 METDST: Vp1 IPCP: PrimaryDNS 10.11.12.13 (0x81060A0B0C0D)

Apr 15 11:47:28.487 METDST: Vp1 IPCP: SecondaryDNS 10.11.12.14 (0x83060A0B0C0E)

Apr 15 11:47:28.487 METDST: Vp1 IPCP: O CONFREQ [REQsent] id 2 len 10
Apr 15 11:47:28.487 METDST: Vp1 IPCP: Address 0.0.0.0 (0x030600000000)
Apr 15 11:47:28.487 METDST: Vp1 IPCP: Event[Receive ConfNak/Rej] State[REQsent to REQsent]
Apr 15 11:47:29.507 METDST: Vp1 PPP: I pkt type 0x8021, datagramsize 18 link[ip]
Apr 15 11:47:29.507 METDST: Vp1 IPCP: I CONFNAK [REQsent] id 2 len 16
Apr 15 11:47:29.507 METDST: Vp1 IPCP: PrimaryDNS 10.11.12.13 (0x81060A0B0C0D)
Apr 15 11:47:29.507 METDST: Vp1 IPCP: SecondaryDNS 10.11.12.14 (0x83060A0B0C0E)
Apr 15 11:47:29.507 METDST: Vp1 IPCP: O CONFREQ [REQsent] id 3 len 10
Apr 15 11:47:29.507 METDST: Vp1 IPCP: Address 0.0.0.0 (0x030600000000)
Apr 15 11:47:29.507 METDST: Vp1 IPCP: Event[Receive ConfNak/Rej] State[REQsent to REQsent]
Apr 15 11:47:30.135 METDST: Vp1 PPP: I pkt type 0x8021, datagramsize 6 link[ip]
Apr 15 11:47:30.135 METDST: Vp1 IPCP: I CONFREQ [REQsent] id 5 len 4
Apr 15 11:47:30.135 METDST: Vp1 **IPCP AUTHOR: Done. Her address 0.0.0.0, we want 0.0.0.0**
Apr 15 11:47:30.135 METDST: Vp1 IPCP: O CONFACK [REQsent] id 5 len 4
Apr 15 11:47:30.135 METDST: Vp1 IPCP: Event[Receive ConfReq+] State[REQsent to ACKsent]
Apr 15 11:47:30.139 METDST: Vp1 PPP: I pkt type 0x8021, datagramsize 12 link[ip]
Apr 15 11:47:30.139 METDST: Vp1 IPCP: I CONFNAK [ACKsent] id 3 len 10
Apr 15 11:47:30.139 METDST: Vp1 IPCP: **Address 10.148.18.193 (0x03060A9412C1)**
Apr 15 11:47:30.139 METDST: Vp1 IPCP: O CONFREQ [ACKsent] id 4 len 10
Apr 15 11:47:30.139 METDST: Vp1 IPCP: Address 10.148.18.193 (0x03060A9412C1)
Apr 15 11:47:30.139 METDST: Vp1 IPCP: Event[Receive ConfNak/Rej] State[ACKsent to ACKsent]
Apr 15 11:47:30.155 METDST: Vp1 PPP: I pkt type 0x8021, datagramsize 12 link[ip]
Apr 15 11:47:30.155 METDST: Vp1 IPCP: I CONFACK [ACKsent] id 4 len 10
Apr 15 11:47:30.155 METDST: Vp1 IPCP: Address 10.148.18.193 (0x03060A9412C1)
Apr 15 11:47:30.155 METDST: Vp1 IPCP: Event[Receive ConfAck] State[ACKsent to Open]
Apr 15 11:47:30.183 METDST: Vp1 IPCP: State is Open
Apr 15 11:47:30.183 METDST: Vp1 IPCP: **Install negotiated IP interface address 10.148.18.193**
Apr 15 11:47:31.971 METDST: Vp1 PPP: I pkt type 0x0021, datagramsize 124 link[ip]
Apr 15 11:47:37.447 METDST: Vp1 LCP: O ECHOREQ [Open] id 1 len 12 magic 0x73D9CC13
Apr 15 11:47:37.455 METDST: Vp1 LCP-FS: I ECHOREP [Open] id 1 len 16 magic 0x011873FC
Apr 15 11:47:37.455 METDST: Vp1 LCP-FS: Received id 1, sent id 1, line up

Comprobamos que el interfaz virtual-ppp1 tiene la IP 10.148.18.193 tal y como indica la traza. Esto verifica que se ha autenticado correctamente contra el radius Converv11 puesto que esta provisionado el usuario y password correctamente y que la sesión PPP obviamente esta establecida correctamente.

Oficina_Movil#sh ip inter brief
Interface IP-Address OK? Method Status Protocol

ATM0	unassigned	YES NVRAM	administratively down	down
Ethernet0	unassigned	YES NVRAM	administratively down	down
FastEthernet0	unassigned	YES unset	down	down
FastEthernet1	unassigned	YES unset	down	down
FastEthernet2	unassigned	YES unset	down	down
FastEthernet3	unassigned	YES unset	up	up
Loopback55	10.95.246.200	YES NVRAM	up	up
Loopback600	10.222.131.220	YES NVRAM	up	up
Tunnel1	10.21.34.34	YES NVRAM	up	down
Tunnel2	10.21.34.50	YES NVRAM	up	down
Virtual-PPP1	**10.148.18.193**	**YES IPCP**	**up**	**up**
Vlan1	unassigned	YES unset	administratively down	down
Vlan19	10.100.100.1	YES NVRAM	up	up
Vlan20	10.22.200.1	YES NVRAM	down	down

8.6 Comprobación de llamada efectuada en el log del radius Conserv11

Si accedemos al radius Conserv11 de Telefónica y buscamos en su Log las llamadas que ha realizado el router por el **número de móvil (676399391) o por el nombre de usuario 1726_sucursal156 veremos que el login se realiza correctamente y en la respuesta le indica la IP (10.148.18.193) que se configurara en el interfaz virtual-ppp1**. A continuación se muestran las trazas del log del radius:

conserv11:/logs/NR_Conmutado $gzip -dc log150414*.gz | grep 1726_sucursal156

2014/04/15 11:37:52.016 <engine.worker.3> |2014/04/15 11:37:52|**1726_sucursal156@vpn-mv-acc-caja-1726**|10.200.13.245|2836749237|||34**676399391**|acc-caja 1726.movistar.es|||||Sync|||arc|**auth|login ok**

2014/04/15 11:37:52.055 <engine.worker.8> |2014/04/15 11:37:52|1726_sucursal156@vpn-mv-acc-caja-1726|10.200.13.245|2836749237|||34676399391|acc-caja-1726.movistar.es|||||Sync|||tme|||**10.148.18.193**|arc|||**started session**

conserv11:/logs/NR_Conmutado $

8.7 Montaje tuneles GRE contra los POI

Partiendo de la situación de que el interfaz virtual-ppp1 ya esta levantado y tiene asignada la IP que le indico previamente el radius Conserv11 a GGSN, **los túneles GRE que encapsulan el trafico IP contra los POI de la red IP Única levantaran puesto que la**

IP origen del túnel GRE (10.148.18.193) coincide con la IP que acaba de ser asignada al interfaz virtual-ppp1.

```
Oficina_Movil#sh ip inter brief
Interface              IP-Address      OK? Method Status                Protocol
ATM0                   unassigned      YES NVRAM  administratively down down
Ethernet0              unassigned      YES NVRAM  administratively down down
FastEthernet0          unassigned      YES unset  down                  down
FastEthernet1          unassigned      YES unset  down                  down
FastEthernet2          unassigned      YES unset  down                  down
FastEthernet3          unassigned      YES unset  up                    up
Loopback55             10.95.246.200   YES NVRAM  up                    up
Loopback600            10.222.131.220  YES NVRAM  up                    up
Tunnel1                10.21.34.34     YES NVRAM  up                    down
Tunnel2                10.21.34.50     YES NVRAM  up                    down
Virtual-PPP1           10.148.18.193   YES IPCP   up                    up
Vlan1                  unassigned      YES unset  administratively down down
Vlan19                 10.100.100.1    YES NVRAM  up                    up
Vlan20                 10.22.200.1     YES NVRAM  down                  down
```

Los interfaces tunnel pasan de down a up:

```
Oficina_Movil#sh ip inter brief
Interface              IP-Address      OK? Method Status                Protocol
ATM0                   unassigned      YES NVRAM  administratively down down
Ethernet0              unassigned      YES NVRAM  administratively down down
FastEthernet0          unassigned      YES unset  down                  down
FastEthernet1          unassigned      YES unset  down                  down
FastEthernet2          unassigned      YES unset  down                  down
FastEthernet3          unassigned      YES unset  up                    up
Loopback55             10.95.246.200   YES NVRAM  up                    up
Loopback600            10.222.131.220  YES NVRAM  up                    up
Tunnel1                10.21.34.34     YES NVRAM  up                    up
Tunnel2                10.21.34.50     YES NVRAM  up                    up
Virtual-PPP1           10.148.18.193   YES IPCP   up                    up
Vlan1                  unassigned      YES unset  administratively down down
Vlan19                 10.100.100.1    YES NVRAM  up                    up
```

Vlan20 10.22.200.1 YES NVRAM down down

Mediante el mandato debug tunnel comprobamos la secuencia en el que se establece los túneles y como encapsula y desencapsula el trafico que se envía y se recibe a través de los interfaces tunnel1 y 2.

Apr 15 12:31:22.363 METDST: %LINEPROTO-5-UPDOWN: Line protocol on Interface **Virtual-PPP1, changed state to up**

Apr 15 12:31:35.175 METDST: FIBtunnel: Tunnel2 physical idb changed from Virtual-PPP1 to Virtual-PPP1

Apr 15 12:31:35.175 METDST: FIBtunnel: Tunnel1 physical idb changed from Virtual-PPP1 to Virtual-PPP1

Apr 15 12:31:35.179 METDST: %LINEPROTO-5-UPDOWN: Line protocol on Interface **Tunnel2,** changed state to **up**

Apr 15 12:31:35.179 METDST: **FIBtunnel: Tu2: stacking IP 0.0.0.0 to Default:172.19.136.129**

Apr 15 12:31:35.179 METDST: %LINEPROTO-5-UPDOWN: Line protocol on Interface **Tunnel1,** changed state to **up**

Apr 15 12:31:35.179 METDST: **FIBtunnel: Tu1: stacking IP 0.0.0.0 to Default:172.19.136.61**

Apr 15 12:31:35.187 METDST: Tunnel1: **GRE/IP encapsulated 10.148.18.193->172.19.136.61** (linktype=7, len=166)

Apr 15 12:31:35.187 METDST: Tunnel1 count tx, adding 0 encap bytes

Apr 15 12:31:35.187 METDST: Tunnel1: GRE/IP encapsulated 10.148.18.193->172.19.136.61 (linktype=7, len=166)

Apr 15 12:31:35.187 METDST: Tunnel1 count tx, adding 0 encap bytes

Apr 15 12:31:41.775 METDST: Tunnel1: GRE/IP encapsulated 10.148.18.193->172.19.136.61 (linktype=7, len=68)

Apr 15 12:31:41.775 METDST: Tunnel1 count tx, adding 0 encap bytes

Apr 15 12:31:42.047 METDST: Tunnel1: GRE/IP to **classify 172.19.136.61->10.148.18.193 (tbl=0,"Default" len=68 ttl=57 tos=0x0)**

Apr 15 12:31:42.047 METDST: Tunnel1: GRE/IP (PS) to decaps 172.19.136.61->10.148.18.193 (tbl=0,"default" len=68 ttl=57)

Apr 15 12:31:42.047 METDST: Tunnel1: GRE decapsulated IP packet (linktype=7, len=44)

Apr 15 12:31:42.047 METDST: Tunnel1: GRE/IP encapsulated 10.148.18.193->172.19.136.61 (linktype=7, len=64)

Apr 15 12:31:42.047 METDST: Tunnel1 count tx, adding 0 encap bytes

Apr 15 12:31:42.047 METDST: Tunnel1: GRE/IP encapsulated 10.148.18.193->172.19.136.61 (linktype=7, len=117)

Apr 15 12:31:42.047 METDST: Tunnel1 count tx, adding 0 encap bytes

Apr 15 12:31:42.799 METDST: Tunnel2: GRE/IP encapsulated 10.148.18.193->172.19.136.129 (linktype=7, len=68)

Apr 15 12:31:42.799 METDST: Tunnel2 count tx, adding 0 encap bytes
Apr 15 12:31:42.955 METDST: Tunnel1: GRE/IP to classify 172.19.136.61->10.148.18.193 (tbl=0,"Default" len=123 ttl=57 tos=0x0)
Apr 15 12:31:42.955 METDST: Tunnel1: GRE/IP (PS) to decaps 172.19.136.61->10.148.18.193 (tbl=0,"default" len=123 ttl=57)
Apr 15 12:31:42.955 METDST: Tunnel1: GRE decapsulated IP packet (linktype=7, len=99)

Adicionalmente mediante los mandatos **show interface tunnel1 y show interface tunnel2 veremos entre otras informaciones, que los interfaces han levantado, las IPs origen y destino del túnel, los bits/seg que se esta cursando** y que se esta encapsulando los datagramas IP en el túnel GRE.

Oficina_Movil#show interface tunnel 1
Tunnel1 is up, line protocol is up
Hardware is Tunnel
Description: "Tunel contra NMAMNOR3"
Internet address is 10.21.34.34/30
MTU 17916 bytes, BW 100 Kbit/sec, DLY 50000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation TUNNEL, loopback not set
Keepalive not set
Tunnel source 10.148.18.193, destination 172.19.136.61
Tunnel protocol/transport GRE/IP
Key disabled, sequencing disabled
Checksumming of packets disabled
Tunnel TTL 255, Fast tunneling enabled
Tunnel transport **MTU 1476 bytes**
Tunnel transmit bandwidth 8000 (kbps)
Tunnel receive bandwidth 8000 (kbps)
Last input 00:00:15, output 00:00:15, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 87
Queueing strategy: fifo
Output queue: 0/0 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
3846 packets input, 573696 bytes, 0 no buffer

```
    Received 0 broadcasts (0 IP multicasts)
    0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    5849 packets output, 1908179 bytes, 0 underruns
    0 output errors, 0 collisions, 0 interface resets
    0 unknown protocol drops
    0 output buffer failures, 0 output buffers swapped out
Oficina_Movil#sh inter tunnel 2
Tunnel2 is up, line protocol is up
  Hardware is Tunnel
  Description: "Tunel contra NMABLLA3(bck)"
  Internet address is 10.21.34.50/30
  MTU 17916 bytes, BW 100 Kbit/sec, DLY 50000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 10.148.18.193, destination 172.19.136.129
  Tunnel protocol/transport GRE/IP
    Key disabled, sequencing disabled
    Checksumming of packets disabled
  Tunnel TTL 255, Fast tunneling enabled
  Tunnel transport MTU 1476 bytes
  Tunnel transmit bandwidth 8000 (kbps)
  Tunnel receive bandwidth 8000 (kbps)
  Last input 00:00:16, output 00:00:16, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 44
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     1074 packets input, 384528 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     1476 packets output, 261939 bytes, 0 underruns
```

0 output errors, 0 collisions, 0 interface resets

0 unknown protocol drops

0 output buffer failures, 0 output buffers swapped out

8.8 Establecimiento sesiones BGP con los POI

Como se ha comentado anteriormente para **anunciar las redes de la oficina móvil hacia la RPV de Caser se emplea routing dinámico mediante el protocolo BGP**. En concreto eBGP puesto son diferentes sistemas autónomos los que **emplea la oficina móvil (65000) frente al de los POI (3352)** que es el sistema autónomo que emplean todos los router de la red IP Única. **Para establecerse la vecindad entre la oficina móvil y los POI los se emplean los interfaces tunel1 y 2, como dichos interfaces ya están levantados a través de ellos se intercambian número de la versión de BGP**, sistema autónomo (AS) y el router ID. Se intercambiaran mensajes pasando por lo que se conoce como estado de los vecinos que corresponde al siguiente diagrama:

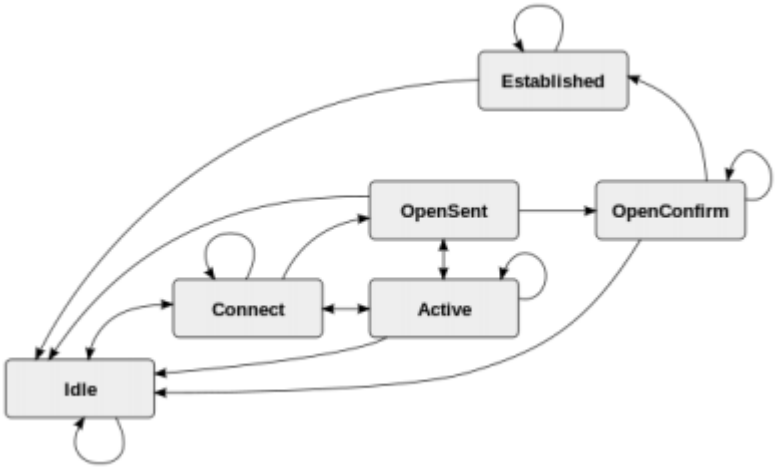


Figura 8.8.9 Diagrama de estados por los que pasa el protocolo BGP.

En la traza se puede comprobar que pasa de estado Idle-> Active-> OpenSent -> OpenConfirm-> Established y por ultimo levantara la sesión BGP. En estado Established la oficina móvil y los **POI comenzaran a intercambiarse los prefijos y la tabla de rutas que conoce la oficina y todas las redes de la RPV de Caser entre ellas la red 10.11.43.0/24** en la que se encuentra el servidor de monitorización (10.11.43.29). En esta traza se observa el dialogo con el POI principal 10.21.34.33:

Apr 15 12:39:16.435 METDST: BGP: 10.21.34.33 active went from **Idle to Active**

Apr 15 12:39:16.435 METDST: BGP: 10.21.34.33 open active, local address 10.21.34.34

Apr 15 12:39:16.507 METDST: BGP: ses global 10.21.34.33 (0x853064C4:0) act Adding topology IPv4 Unicast:base

Apr 15 12:39:16.507 METDST: BGP: ses global 10.21.34.33 (0x853064C4:0) act Send OPEN

Apr 15 12:39:16.507 METDST: BGP: **10.21.34.33 active went from Active to OpenSent**

Apr 15 12:39:16.507 METDST: BGP: 10.21.34.33 active sending OPEN, version 4, my as: 65000, holdtime 180 seconds, ID ADE83DC

Apr 15 12:39:16.695 METDST: BGP: 10.21.34.33 active rcv message type 1, length (excl. header) 40

Apr 15 12:39:16.695 METDST: BGP: ses global 10.21.34.33 (0x853064C4:0) act Receive OPEN

Apr 15 12:39:16.695 METDST: BGP: 10.21.34.33 active rcv OPEN, version 4, holdtime 90 seconds

Apr 15 12:39:16.695 METDST: BGP: 10.21.34.33 active rcv OPEN w/ OPTION parameter len: 30

Apr 15 12:39:16.695 METDST: BGP: 10.21.34.33 active rcvd OPEN w/ optional parameter type 2 (Capability) len 6

Apr 15 12:39:16.695 METDST: BGP: 10.21.34.33 active OPEN has CAPABILITY code: 1, length 4

Apr 15 12:39:16.695 METDST: BGP: 10.21.34.33 active OPEN has MP_EXT CAP for afi/safi: 1/1

Apr 15 12:39:16.695 METDST: BGP: 10.21.34.33 active rcvd OPEN w/ optional parameter type 2 (Capability) len 2

Apr 15 12:39:16.695 METDST: BGP: 10.21.34.33 active OPEN has CAPABILITY code: 128, length 0

Apr 15 12:39:16.695 METDST: BGP: 10.21.34.33 active OPEN has ROUTE-REFRESH capability(old) for all address-families

Apr 15 12:39:16.695 METDST: BGP: 10.21.34.33 active rcvd OPEN w/ optional parameter type 2 (Capability) len 2

Apr 15 12:39:16.699 METDST: BGP: 10.21.34.33 active OPEN has CAPABILITY code: 2, length 0

Apr 15 12:39:16.699 METDST: BGP: 10.21.34.33 active OPEN has ROUTE-REFRESH capability(new) for all address-families

Apr 15 12:39:16.699 METDST: BGP: 10.21.34.33 active rcvd OPEN w/ optional parameter type 2 (Capability) len 4

Apr 15 12:39:16.699 METDST: BGP: 10.21.34.33 active OPEN has CAPABILITY code: 64, length 2

Apr 15 12:39:16.699 METDST: BGP: ses global 10.21.34.33 (0x853064C4:0) act NSF OPEN has GR cap

Apr 15 12:39:16.699 METDST: BGP: ses global 10.21.34.33 (0x853064C4:0) act NSF Peer has not restarted. Restart Time: 120

Apr 15 12:39:16.699 METDST: BGP: 10.21.34.33 active rcvd OPEN w/ optional parameter type 2 (Capability) len 6

Apr 15 12:39:16.699 METDST: BGP: 10.21.34.33 active OPEN has CAPABILITY code: 65, length 4

Apr 15 12:39:16.699 METDST: BGP: 10.21.34.33 active OPEN has 4-byte ASN CAP for: 3352

Apr 15 12:39:16.699 METDST: BGP: nbr global 10.21.34.33 neighbor does not have IPv4 MDT topology activated

Apr 15 12:39:16.699 METDST: BGP: 10.21.34.33 active rcvd OPEN w/ remote AS 3352, 4-byte remote AS 3352
Apr 15 12:39:16.699 METDST: BGP: **10.21.34.33 active went from OpenSent to OpenConfirm**
Apr 15 12:39:16.807 METDST: BGP**: 10.21.34.33 active went from OpenConfirm to Established**
Apr 15 12:39:16.807 METDST: BGP: ses global 10.21.34.33 (0x853064C4:1) act Assigned ID
Apr 15 12:39:16.807 METDST: BGP: ses global 10.21.34.33 (0x853064C4:1) Up
Apr 15 12:39:16.807 METDST: %BGP-5-ADJCHANGE: **neighbor 10.21.34.33 Up**

Y esta seria la traza para el establecimiento de la vecindad con el POI de backup 10.21.34.49:

Apr 15 12:39:17.459 METDST: BGP: **10.21.34.49 active went from Idle to Active**
Apr 15 12:39:17.459 METDST: BGP: 10.21.34.49 open active, local address 10.21.34.50
Apr 15 12:39:17.567 METDST: BGP: ses global 10.21.34.49 (0x87B3E1C4:0) act Adding topology IPv4 Unicast:base
Apr 15 12:39:17.567 METDST: BGP: ses global 10.21.34.49 (0x87B3E1C4:0) act Send OPEN
Apr 15 12:39:17.567 METDST: BGP: **10.21.34.49 active went from Active to OpenSent**
Apr 15 12:39:17.567 METDST: BGP: 10.21.34.49 active sending OPEN, version 4, my as: 65000, holdtime 180 seconds, ID ADE83DC
Apr 15 12:39:17.647 METDST: BGP: 10.21.34.49 active rcv message type 1, length (excl. header) 40
Apr 15 12:39:17.647 METDST: BGP: ses global 10.21.34.49 (0x87B3E1C4:0) act Receive OPEN
Apr 15 12:39:17.647 METDST: BGP: 10.21.34.49 active rcv OPEN, version 4, holdtime 90 seconds
Apr 15 12:39:17.647 METDST: BGP: 10.21.34.49 active rcv OPEN w/ OPTION parameter len: 30
Apr 15 12:39:17.647 METDST: BGP: 10.21.34.49 active rcvd OPEN w/ optional parameter type 2 (Capability) len 6
Apr 15 12:39:17.647 METDST: BGP: 10.21.34.49 active OPEN has CAPABILITY code: 1, length 4
Apr 15 12:39:17.647 METDST: BGP: 10.21.34.49 active OPEN has MP_EXT CAP for afi/safi: 1/1
Apr 15 12:39:17.647 METDST: BGP: 10.21.34.49 active rcvd OPEN w/ optional parameter type 2 (Capability) len 2
Apr 15 12:39:17.647 METDST: BGP: 10.21.34.49 active OPEN has CAPABILITY code: 128, length 0
Apr 15 12:39:17.647 METDST: BGP: 10.21.34.49 active OPEN has ROUTE-REFRESH capability(old) for all address-families
Apr 15 12:39:17.647 METDST: BGP: 10.21.34.49 active rcvd OPEN w/ optional parameter type 2 (Capability) len 2
Apr 15 12:39:17.647 METDST: BGP: 10.21.34.49 active OPEN has CAPABILITY code: 2, length 0
Apr 15 12:39:17.647 METDST: BGP: 10.21.34.49 active OPEN has ROUTE-REFRESH capability(new) for all address-families
Apr 15 12:39:17.647 METDST: BGP: 10.21.34.49 active rcvd OPEN w/ optional parameter type 2 (Capability) len 4

Apr 15 12:39:17.647 METDST: BGP: 10.21.34.49 active OPEN has CAPABILITY code: 64, length 2
Apr 15 12:39:17.647 METDST: BGP: ses global 10.21.34.49 (0x87B3E1C4:0) act NSF OPEN has GR cap
Apr 15 12:39:17.647 METDST: BGP: ses global 10.21.34.49 (0x87B3E1C4:0) act NSF Peer has not restarted. Restart Time: 120
Apr 15 12:39:17.647 METDST: BGP: 10.21.34.49 active rcvd OPEN w/ optional parameter type 2 (Capability) len 6
Apr 15 12:39:17.647 METDST: BGP: 10.21.34.49 active OPEN has CAPABILITY code: 65, length 4
Apr 15 12:39:17.647 METDST: BGP: 10.21.34.49 active OPEN has 4-byte ASN CAP for: 3352
Apr 15 12:39:17.647 METDST: BGP: nbr global 10.21.34.49 neighbor does not have IPv4 MDT topology activated
Apr 15 12:39:17.647 METDST: BGP: 10.21.34.49 active rcvd OPEN w/ remote AS 3352, 4-byte remote AS 3352
Apr 15 12:39:17.647 METDST: BGP: **10.21.34.49 active went from OpenSent to OpenConfirm**
Apr 15 12:39:17.715 METDST: BGP: **10.21.34.49 active went from OpenConfirm to Established**
Apr 15 12:39:17.715 METDST: BGP: ses global 10.21.34.49 (0x87B3E1C4:1) act Assigned ID
Apr 15 12:39:17.715 METDST: BGP: ses global 10.21.34.49 (0x87B3E1C4:1) Up
Apr 15 12:39:17.715 METDST: %**BGP-5-ADJCHANGE: neighbor 10.21.34.49 Up**

Mediante el mandato **show ip bgp summary** vemos que se están intercambiando prefijos con los POI y que las sesiones llevan levantadas una duración de tiempo:

Oficina_Movil#show ip bgp summary
BGP router identifier 10.222.131.220, local AS **number 65000**
BGP table version is 13940, main routing table version 13940
396 network entries using 53856 bytes of memory
788 path entries using 44128 bytes of memory
404/137 BGP path/bestpath attribute entries using 51712 bytes of memory
3 BGP AS-PATH entries using 72 bytes of memory
112 BGP extended community entries using 3104 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 152872 total bytes of memory
BGP activity 4726/4330 prefixes, 11000/10212 paths, scan interval 60 secs

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
10.21.34.33	4	3352	342	13	13940	0	0	**00:03:08**	**392**
10.21.34.49	4	3352	338	146	13940	0	0	**00:03:07**	**392**

Con el mandato **show ip bgp neighbors** se da información mas especifica de la sesión BGP establecida.

Características de la sesión BGP con el POI PRINCIPAL:

```
Oficina_Movil#show ip bgp neighbors
BGP neighbor is 10.21.34.33,  remote AS 3352, external link
 BGP version 4, remote router ID 172.19.136.61
 BGP state = Established, up for 00:03:13
 Last read 00:00:20, last write 00:00:25, hold time is 90, keepalive interval is 30 seconds
 Neighbor sessions:
  1 active, is not multisession capable (disabled)
  Session: 10.21.34.33
   Topology IPv4 Unicast
 Neighbor capabilities:
  Route refresh: advertised and received(new)
  Four-octets ASN Capability: advertised and received
  Address family IPv4 Unicast: advertised and received
  Graceful Restart Capability: received
   Remote Restart timer is 120 seconds
   Address families advertised by peer:
    none
  Multisession Capability:
 Message statistics:
  InQ depth is 0
  OutQ depth is 0
                Sent       Rcvd
  Opens:           1          1
  Notifications:   0          0
  Updates:         4        333
  Keepalives:      8          8
  Route Refresh:   0          0
  Total:          13        342
 Default minimum time between advertisement runs is 30 seconds
```

Características de la sesión BGP con el POI BACKUP:

```
BGP neighbor is 10.21.34.49,  remote AS 3352, external link
 BGP version 4, remote router ID 172.19.136.129
 BGP state = Established, up for 00:03:12
 Last read 00:00:19, last write 00:00:02, hold time is 90, keepalive interval is 30 seconds
 Neighbor sessions:
  1 active, is not multisession capable (disabled)
  Session: 10.21.34.49
   Topology IPv4 Unicast
 Neighbor capabilities:
  Route refresh: advertised and received(new)
  Four-octets ASN Capability: advertised and received
  Address family IPv4 Unicast: advertised and received
  Graceful Restart Capability: received
   Remote Restart timer is 120 seconds
   Address families advertised by peer:
    none
  Multisession Capability:
 Message statistics:
  InQ depth is 0
  OutQ depth is 0
                Sent       Rcvd
  Opens:            1          1
  Notifications:    0          0
  Updates:        137        329
  Keepalives:       9          8
  Route Refresh:    0          0
  Total:          147        338
 Default minimum time between advertisement runs is 30 seconds
```

Mediante el mandato **show ip bgp y show ip route** comprobamos que la oficina movil ya comienza a recibir redes via bgp perteneciente a la RPV de Caser entre ellas la red 10.7.43.0/24

```
Oficina_Movil#sh ip bgp
BGP table version is 13940, local router ID is 10.222.131.220
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
```

```
        r RIB-failure, S Stale, m multipath, b backup-path, x best-external, f RT-Filter
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*  10.8.0.0/23      10.21.34.49              100      0 3352 3352 ?
*>                  10.21.34.33              150      0 3352 3352 ?
*  10.11.0.0/16     10.21.34.49              100      0 3352 3352 ?
*>                  10.21.34.33              150      0 3352 3352 ?
*  10.18.0.0/23     10.21.34.49              100      0 3352 3352 ?
*>                  10.21.34.33              150      0 3352 3352 ?
*  10.19.0.0/16     10.21.34.49              100      0 3352 3352 ?
*>                  10.21.34.33              150      0 3352 3352 ?
*  10.20.3.0/24     10.21.34.49              100      0 3352 3352 ?
*>                  10.21.34.33              150      0 3352 3352 ?
*  10.20.6.0/24     10.21.34.49              100      0 3352 3352 ?
*>                  10.21.34.33              150      0 3352 3352 ?
*  10.20.9.0/24     10.21.34.49              100      0 3352 3352 i
*>                  10.21.34.33              150      0 3352 3352 i
*  10.20.10.0/24    10.21.34.49              100      0 3352 3352 i
*>                  10.21.34.33              150      0 3352 3352 i
```

```
Oficina_Movil#sh ip route 10.11.43.0
Routing entry for 10.7.43.0/24
  Known via "bgp 65000", distance 20, metric 0
  Tag 3352, type external
  Last update from 10.21.34.33 00:03:27 ago
  Routing Descriptor Blocks:
  * 10.21.34.33, from 10.21.34.33, 00:03:27 ago
      Route metric is 0, traffic share count is 1
      AS Hops 2
      Route tag 3352
      MPLS label: none
```

Con el mandato **show ip bgp neighbors 10.21.34.33 advertised-routes** indicamos que redes estamos anunciando de la oficina móvil a los POIs para que el servidor de monitorización sepa alcanzar el portátil de la oficina móvil.

```
Oficina_Movil#sh ip bgp neighbors 10.21.34.33 advertised-routes
BGP table version is 424, local router ID is 10.222.131.220
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, x best-external, f RT-Filter
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 10.22.200.0/24   0.0.0.0                  0         32768 i
*> 10.95.246.200/32 0.0.0.0                  0         32768 i
*> 172.19.136.128/30
                    10.21.34.49            100      0 3352 i
*> 172.29.29.200/32 0.0.0.0                  0         32768 i

Total number of prefixes 4
```

8.9 Cifrado del tráfico mediante túneles IPSEC

Para el montaje del túnel IPSEC entre el router de oficinas y el router central y cifrar el tráfico que se cursa entre ambas sedes empleando la red IP Única es necesario que se conozca en la tabla de rutas del router de la oficina móvil la IP del peer del túnel IPSEC del router central. Para ello comprobamos mediante el mandato **show ip route 10.95.246.2 que conocemos la red en nuestra tabla de rutas.**

```
Oficina_Movil#sh ip route 10.95.246.2
Routing entry for 10.95.246.2/32
  Known via "bgp 65000", distance 20, metric 0
  Tag 3352, type external
  Last update from 10.21.34.33 00:03:48 ago
  Routing Descriptor Blocks:
  * 10.21.34.33, from 10.21.34.33, 00:03:48 ago
      Route metric is 0, traffic share count is 1
      AS Hops 2
      Route tag 3352
      MPLS label: none
```

Comprobamos que tenemos conectividad IP con la IP túnel IPSEC de la sede central poniendo como origen la ip del tunel de IPSEC de la oficina movil.

Oficina_Movil#ping 10.95.246.2 source loopback 55
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.95.246.2, timeout is 2 seconds:
Packet sent with a source address of 10.95.246.200
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/57/60 ms

Verificada la conectividad entre ambos peers para que se monte el túnel se tiene que generar tráfico que cumpla el criterio de cifrado. Dado que lo que queremos cifrar es el trafico que va con origen la red 10.22.200/24 a la red del servidor de monitorización 10.11.43.0/24 basara **con lanzar un ping desde el portátil de pruebas al servidor para que cumpla la condición y se negocie y se monte el túnel IPSEC entre ambos routers**.Con el mandato **show access-list 2699** vemos que las coincidencias (matches) van aumentando por lo que cumple la condicion de cifrado:

Oficina_Movil# show access-lists **2699**
Extended IP access list 2699
10 permit ip 10.22.200.0 0.0.0.255 10.7.43.0 0.0.0.255 **(39 matches)**

Mediante los mandatos **debug crypto isakmap y debug crypto ipsec** se puede comprobar **las fases de negociación (reconocimiento y aceptación de los equipos origen y destino como equipos capaces de cifrar, desencadena la negociación de la sesión IKE (ISAKMP),** la asociación de seguridad entre 2 entidades (SA de IPSec) y por ultimo la sesión IPSEC que se emplea para cifrar los datagramas IP.

Apr 15 15:01:01.658 METDST: ISAKMP:(0):found peer pre-shared key matching **10.95.246.2**
Apr 15 15:01:01.658 METDST: ISAKMP:(0): constructed NAT-T vendor-rfc3947 ID
Apr 15 15:01:01.658 METDST: ISAKMP:(0): constructed NAT-T vendor-07 ID
Apr 15 15:01:01.658 METDST: ISAKMP:(0): constructed NAT-T vendor-03 ID
Apr 15 15:01:01.658 METDST: ISAKMP:(0): constructed NAT-T vendor-02 ID
Apr 15 15:01:01.658 METDST: ISAKMP:(0):Input = IKE_MESG_FROM_IPSEC, IKE_SA_REQ_MM

Apr 15 15:01:01.658 METDST: ISAKMP:(0):Old State = IKE_READY New State = IKE_I_MM1

Apr 15 15:01:01.658 METDST: ISAKMP:(0): beginning Main Mode exchange
Apr 15 15:01:01.658 METDST: ISAKMP:(0): **sending packet to 10.95.246.2 my_port 500 peer_port 500 (I) MM_NO_STATE**
Apr 15 15:01:01.658 METDST: ISAKMP:(0):Sending an IKE IPv4 Packet.
Apr 15 15:01:02.462 METDST: ISAKMP (0): received packet from 10.95.246.2 dport 500 sport 500 Global (I) MM_NO_STATE
Apr 15 15:01:02.462 METDST: ISAKMP:(0):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
Apr 15 15:01:02.462 METDST: ISAKMP:(0):Old State = IKE_I_MM1 New State = IKE_I_MM2

Apr 15 15:01:02.462 METDST: ISAKMP:(0): processing SA payload. message ID = 0
Apr 15 15:01:02.462 METDST: ISAKMP:(0): processing vendor id payload
Apr 15 15:01:02.462 METDST: ISAKMP:(0): vendor ID seems Unity/DPD but major 69 mismatch
Apr 15 15:01:02.462 METDST: ISAKMP (0): vendor ID is NAT-T RFC 3947
Apr 15 15:01:02.462 METDST: ISAKMP:(0):found peer pre-shared key matching 10.95.246.2
Apr 15 15:01:02.462 METDST: ISAKMP:(0): local preshared key found
Apr 15 15:01:02.462 METDST: ISAKMP : Scanning profiles for xauth ...
Apr 15 15:01:02.466 METDST: ISAKMP:(0):Checking ISAKMP transform 1 against priority 10 policy
Apr 15 15:01:02.466 METDST: ISAKMP: **encryption 3DES-CBC**
Apr 15 15:01:02.466 METDST: ISAKMP: **hash MD5**
Apr 15 15:01:02.466 METDST: ISAKMP: **default group 1**
Apr 15 15:01:02.466 METDST: ISAKMP: **auth pre-share**
Apr 15 15:01:02.466 METDST: ISAKMP: **life type in seconds**
Apr 15 15:01:02.466 METDST: ISAKMP**:** **life duration (basic) of 21600**
Apr 15 15:01:02.466 METDST: ISAKMP:(0):atts are acceptable. Next payload is 0
Apr 15 15:01:02.466 METDST: ISAKMP:(0):Acceptable atts:actual life: 0
Apr 15 15:01:02.466 METDST: ISAKMP:(0):Acceptable atts:life: 0
Apr 15 15:01:02.466 METDST: ISAKMP:(0):Basic life_in_seconds:21600
Apr 15 15:01:02.466 METDST: ISAKMP:(0):Returning Actual lifetime: 21600
Apr 15 15:01:02.466 METDST: ISAKMP:(0)::Started lifetime timer: 21600.

Apr 15 15:01:02.466 METDST: ISAKMP:(0): processing vendor id payload
Apr 15 15:01:02.466 METDST: ISAKMP:(0): vendor ID seems Unity/DPD but major 69 mismatch
Apr 15 15:01:02.466 METDST: ISAKMP (0): vendor ID is NAT-T RFC 3947
Apr 15 15:01:02.466 METDST: ISAKMP:(0):Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE
Apr 15 15:01:02.466 METDST: ISAKMP:(0):Old State = IKE_I_MM2 New State = IKE_I_MM2

Apr 15 15:01:02.466 METDST: ISAKMP:(0): sending packet to 10.95.246.2 my_port 500 peer_port 500 (I) MM_SA_SETUP
Apr 15 15:01:02.466 METDST: ISAKMP:(0):Sending an IKE IPv4 Packet.
Apr 15 15:01:02.466 METDST: ISAKMP:(0):Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE
Apr 15 15:01:02.466 METDST: ISAKMP:(0):Old State = IKE_I_MM2 New State = IKE_I_MM3

Apr 15 15:01:02.622 METDST: ISAKMP (0): received packet from 10.95.246.2 dport 500 sport 500 Global (I) MM_SA_SETUP
Apr 15 15:01:02.622 METDST: ISAKMP:(0):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
Apr 15 15:01:02.622 METDST: ISAKMP:(0):Old State = IKE_I_MM3 New State = IKE_I_MM4

Apr 15 15:01:02.622 METDST: ISAKMP:(0): processing KE payload. message ID = 0
Apr 15 15:01:02.642 METDST: ISAKMP:(0): processing NONCE payload. message ID = 0
Apr 15 15:01:02.642 METDST: ISAKMP:(0):found peer pre-shared key matching 10.95.246.2
Apr 15 15:01:02.642 METDST: ISAKMP:(2003): processing vendor id payload
Apr 15 15:01:02.642 METDST: ISAKMP:(2003): vendor ID is Unity
Apr 15 15:01:02.642 METDST: ISAKMP:(2003): processing vendor id payload
Apr 15 15:01:02.642 METDST: ISAKMP:(2003): vendor ID is DPD
Apr 15 15:01:02.642 METDST: ISAKMP:(2003): processing vendor id payload
Apr 15 15:01:02.642 METDST: ISAKMP:(2003): speaking to another IOS box!
Apr 15 15:01:02.642 METDST: ISAKMP:received payload type 20
Apr 15 15:01:02.642 METDST: ISAKMP (2003): His hash no match - this node outside NAT
Apr 15 15:01:02.642 METDST: ISAKMP:received payload type 20
Apr 15 15:01:02.642 METDST: ISAKMP (2003): No NAT Found for self or peer
Apr 15 15:01:02.642 METDST: ISAKMP:(2003):Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE

Apr 15 15:01:02.642 METDST: ISAKMP:(2003):Old State = IKE_I_MM4 New State = IKE_I_MM4

Apr 15 15:01:02.642 METDST: ISAKMP:(2003):Send initial contact
Apr 15 15:01:02.642 METDST: ISAKMP:(2003):**SA is doing pre-shared key authentication using id type ID_IPV4_ADDR**
Apr 15 15:01:02.642 METDST: ISAKMP (2003): **ID payload**
next-payload : 8
type : 1
address : 10.95.246.200
protocol : 17
port : 500
length : 12
Apr 15 15:01:02.642 METDST: ISAKMP:(2003):Total payload length: 12
Apr 15 15:01:02.642 METDST: ISAKMP:(2003): sending packet to 10.95.246.2 my_port 500 peer_port 500 (I) MM_KEY_EXCH
Apr 15 15:01:02.642 METDST: ISAKMP:(2003):Sending an IKE IPv4 Packet.
Apr 15 15:01:02.646 METDST: ISAKMP:(2003):Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE
Apr 15 15:01:02.646 METDST: ISAKMP:(2003):Old State = IKE_I_MM4 New State = IKE_I_MM5

Apr 15 15:01:02.714 METDST: ISAKMP (2003): received packet from 10.95.246.2 dport 500 sport 500 Global (I) MM_KEY_EXCH
Apr 15 15:01:02.714 METDST: ISAKMP:(2003): processing ID payload. message ID = 0
Apr 15 15:01:02.714 METDST: ISAKMP (2003): ID payload
next-payload : 8
type : 1
address : 10.95.246.2
protocol : 17
port : 500
length : 12
Apr 15 15:01:02.714 METDST: ISAKMP:(0):: peer matches *none* of the profiles
Apr 15 15:01:02.714 METDST: ISAKMP:(2003): processing HASH payload. message ID = 0
Apr 15 15:01:02.714 METDST: ISAKMP:(2003):SA authentication status:
authenticated

Apr 15 15:01:02.714 METDST: ISAKMP:(2003):SA has been authenticated with 10.95.246.2
Apr 15 15:01:02.714 METDST: ISAKMP: Trying to insert a peer 10.95.246.200/10.95.246.2/500/, and inserted successfully 87A11600.
Apr 15 15:01:02.714 METDST: ISAKMP:(2003):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
Apr 15 15:01:02.714 METDST: ISAKMP:(2003):Old State = IKE_I_MM5 New State = IKE_I_MM6

Apr 15 15:01:02.714 METDST: ISAKMP:(2003):Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE
Apr 15 15:01:02.714 METDST: ISAKMP:(2003):Old State = IKE_I_MM6 New State = IKE_I_MM6

Apr 15 15:01:02.714 METDST: ISAKMP:(2003):Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE
Apr 15 15:01:02.714 METDST: ISAKMP:(2003):Old State = IKE_I_MM6 New State = IKE_P1_COMPLETE

Apr 15 15:01:02.714 METDST: ISAKMP:(2003):IKE_DPD is enabled, initializing timers
Apr 15 15:01:02.714 METDST: ISAKMP:(2003):beginning Quick Mode exchange, M-ID of 2588410962
Apr 15 15:01:02.714 METDST: ISAKMP:(2003):QM Initiator gets spi
Apr 15 15:01:02.718 METDST: ISAKMP:(2003): sending packet to 10.95.246.2 my_port 500 peer_port 500 (I) QM_IDLE
Apr 15 15:01:02.718 METDST: ISAKMP:(2003):Sending an IKE IPv4 Packet.
Apr 15 15:01:02.718 METDST: ISAKMP:(2003):Node 2588410962, Input = IKE_MESG_INTERNAL, IKE_INIT_QM
Apr 15 15:01:02.718 METDST: ISAKMP:(2003):Old State = IKE_QM_READY New State = IKE_QM_I_QM1
Apr 15 15:01:02.718 METDST: ISAKMP:(2003):Input = IKE_MESG_INTERNAL, IKE_PHASE1_COMPLETE
Apr 15 15:01:02.718 METDST: ISAKMP:(2003):Old State = IKE_P1_COMPLETE New State = IKE_P1_COMPLETE

Apr 15 15:01:02.794 METDST: ISAKMP (2003): received packet from 10.95.246.2 dport 500 sport 500 Global (I) QM_IDLE

Apr 15 15:01:02.794 METDST: ISAKMP:(2003): processing HASH payload. message ID = 2588410962

Apr 15 15:01:02.794 METDST: ISAKMP:(2003): processing SA payload. message ID = 2588410962

Apr 15 15:01:02.794 METDST: ISAKMP:(2003):**Checking IPSec proposal 1**

Apr 15 15:01:02.794 METDST: ISAKMP: transform 1, ESP_3DES

Apr 15 15:01:02.794 METDST: ISAKMP: attributes in transform:

Apr 15 15:01:02.794 METDST: ISAKMP: encaps is 1 (Tunnel)

Apr 15 15:01:02.794 METDST: ISAKMP: SA life type in seconds

Apr 15 15:01:02.794 METDST: ISAKMP: SA life duration (basic) of 18000

Apr 15 15:01:02.794 METDST: ISAKMP: SA life type in kilobytes

Apr 15 15:01:02.794 METDST: ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0

Apr 15 15:01:02.794 METDST: ISAKMP: authenticator is HMAC-SHA

Apr 15 15:01:02.794 METDST: ISAKMP:(2003):atts are acceptable.

Apr 15 15:01:02.794 METDST: IPSEC(validate_proposal_request): proposal part #1

Apr 15 15:01:02.794 METDST: IPSEC(validate_proposal_request): proposal part #1,

(key eng. msg.) INBOUND local= 10.95.246.200:0, remote= 10.95.246.2:0,

local_proxy= 10.22.200.0/255.255.255.0/0/0 (type=4),

remote_proxy= 10.7.43.0/255.255.255.0/0/0 (type=4),

protocol= ESP, transform= NONE (Tunnel),

lifedur= 0s and 0kb,

spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x0

Apr 15 15:01:02.794 METDST: Crypto mapdb : proxy_match

src addr : 10.22.200.0

dst addr : 10.7.43.0

protocol : 0

src port : 0

dst port : 0

Apr 15 15:01:02.794 METDST: ISAKMP:(2003): processing NONCE payload. message ID = 2588410962

Apr 15 15:01:02.794 METDST: ISAKMP:(2003): processing ID payload. message ID = 2588410962

Apr 15 15:01:02.794 METDST: ISAKMP:(2003): processing ID payload. message ID = 2588410962

Apr 15 15:01:02.794 METDST: ISAKMP:(2003): **Creating IPSec SAs**

Apr 15 15:01:02.794 METDST: inbound SA from 10.95.246.2 to 10.95.246.200 (f/i) 0/ 0

(proxy 10.7.43.0 to 10.22.200.0)

Apr 15 15:01:02.794 METDST: has spi 0x2341AE83 and conn_id 0

Apr 15 15:01:02.794 METDST: lifetime of 18000 seconds

Apr 15 15:01:02.794 METDST: lifetime of 4608000 kilobytes

Apr 15 15:01:02.794 METDST: outbound SA from 10.95.246.200 to 10.95.246.2 (f/i) 0/0

(proxy 10.22.200.0 to 10.7.43.0)

Apr 15 15:01:02.794 METDST: has spi 0x643C61EB and conn_id 0

Apr 15 15:01:02.794 METDST: lifetime of 18000 seconds

Apr 15 15:01:02.794 METDST: lifetime of 4608000 kilobytes

Apr 15 15:01:02.794 METDST: ISAKMP:(2003): sending packet to 10.95.246.2 my_port 500 peer_port 500 (I) QM_IDLE

Apr 15 15:01:02.794 METDST: ISAKMP:(2003):Sending an IKE IPv4 Packet.

Apr 15 15:01:02.798 METDST: ISAKMP:(2003):deleting node -1706556334 error FALSE reason "No Error"

Apr 15 15:01:02.798 METDST: ISAKMP:(2003):Node 2588410962, Input = IKE_MESG_FROM_PEER, IKE_QM_EXCH

Apr 15 15:01:02.798 METDST: ISAKMP:(2003):Old State = IKE_QM_I_QM1 New State = IKE_QM_PHASE2_COMPLETE

Apr 15 15:01:02.798 METDST: IPSEC(key_engine): got a queue event with 1 KMI message(s)

Apr 15 15:01:02.798 METDST: Crypto mapdb : proxy_match

src addr : 10.22.200.0

dst addr : 10.7.43.0

protocol : 0

src port : 0

dst port : 0

Apr 15 15:01:02.798 METDST: IPSEC(crypto_ipsec_sa_find_ident_head): reconnecting with the same proxies and peer 10.95.246.2

Apr 15 15:01:02.798 METDST: IPSEC(policy_db_add_ident): src 10.22.200.0, dest 10.7.43.0, dest_port 0

Apr 15 15:01:02.798 METDST: IPSEC(create_sa): starting idle timer, 120 seconds

Apr 15 15:01:02.798 METDST: IPSEC(create_sa): sa created,

(sa) sa_dest= 10.95.246.200, sa_proto= 50,

sa_spi= 0x2341AE83(591507075),

sa_trans= esp-3des esp-sha-hmac , sa_conn_id= 5

sa_lifetime(k/sec)= (4601051/18000)

Apr 15 15:01:02.798 METDST: IPSEC(create_sa): sa created,
(sa) sa_dest= 10.95.246.2, sa_proto= 50,
sa_spi= 0x643C61EB(1681678827),
sa_trans= esp-3des esp-sha-hmac , sa_conn_id= 6
sa_lifetime(k/sec)= (4601051/18000)
Apr 15 15:01:02.798 METDST: IPSEC(update_current_outbound_sa): get enable SA peer 10.95.246.2 current outbound sa to SPI 643C61EB
Apr 15 15:01:02.798 METDST: IPSEC(update_current_outbound_sa): updated peer 10.95.246.2 current outbound sa to SPI 643C61EB
Apr 15 15:01:05.554 METDST: BGP: topo global:IPv4 Unicast:base Scanning routing tables
Apr 15 15:01:05.554 METDST: BGP: topo global:IPv4 Multicast:base Scanning routing tables

Con el mandato **show crypto isakmp sa detail** vemos que el túnel esta ACTIVO y que le quedan menos de 6 horas de vida:

Oficina_Movil#show crypto isakmp sa detail
Codes: C - IKE configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal
T - cTCP encapsulation, X - IKE Extended Authentication
psk - Preshared key, rsig - RSA signature
renc - RSA encryption
IPv4 Crypto ISAKMP SA

C-id Local Remote I-VRF Status Encr Hash Auth DH Lifetime Cap.

2004 10.95.246.200 10.95.246.2 **ACTIVE** 3des md5 psk 1 **05:59:27** D

En el lado del router central tambien esta activo el tunel
cajam-sace#sh crypto isa sa
IPv4 Crypto ISAKMP SA
dst src state conn-id status
10.95.246.2 10.95.246.200 QM_IDLE 35122 **ACTIVE**

Y con el mandato **show crypto ipsec sa** vemos las asociaciones de seguridad establecidas, que es una por cada access-list definido entre los peers, en este caso solo un SA por solo existe un access-list. Ademas se observa que ya ha cifrado 7 paquetes que cumplen ese SA.

```
Oficina_Movil#show crypto ipsec sa

interface: Tunnel1
    Crypto map tag: mapacifrado, local addr 10.95.246.200

  protected vrf: (none)
  local  ident (addr/mask/prot/port): (10.22.200.0/255.255.255.0/0/0)
  remote ident (addr/mask/prot/port): (10.7.43.0/255.255.255.0/0/0)
  current_peer 10.95.246.2 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 7, #pkts encrypt: 7, #pkts digest: 7
   #pkts decaps: 7, #pkts decrypt: 7, #pkts verify: 7
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 3, #recv errors 0

    local crypto endpt.: 10.95.246.200, remote crypto endpt.: 10.95.246.2
    path mtu 1476, ip mtu 1476, ip mtu idb Tunnel1
    current outbound spi: 0x643C61EB(1681678827)
    PFS (Y/N): N, DH group: none

    inbound esp sas:
     spi: 0x2341AE83(591507075)
       transform: esp-3des esp-sha-hmac ,
       in use settings ={Tunnel, }
       conn id: 5, flow_id: Onboard VPN:5, sibling_flags 80000046, crypto map: mapacifrado
       sa timing: remaining key lifetime (k/sec): (4601050/17893)
       IV size: 8 bytes
       replay detection support: N
       Status: ACTIVE

    inbound ah sas:

    inbound pcp sas:
```

outbound esp sas:
spi: 0x643C61EB(1681678827)
transform: esp-3des esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 6, flow_id: Onboard VPN:6, sibling_flags 80000046, crypto map: mapacifrado
sa timing: remaining key lifetime (k/sec): (4601050/17893)
IV size: 8 bytes
replay detection support: N
Status: ACTIVE
outbound ah sas:
outbound pcp sas:

8.10 Comprobación conectividad con el servidor monitorización

Lanzamos un ping a la IP del servidor de monitorización (10.11.43.29) que se encuentra en la sede central de Caser de Madrid

```
C:\>ping 10.11.43.29

Haciendo ping a 10.11.43.29 con 32 bytes de datos:

Respuesta desde 10.11.43.29: bytes=32 tiempo=976ms TTL=125
Respuesta desde 10.11.43.29: bytes=32 tiempo=114ms TTL=125
Respuesta desde 10.11.43.29: bytes=32 tiempo=91ms TTL=125
Respuesta desde 10.11.43.29: bytes=32 tiempo=109ms TTL=125

Estadísticas de ping para 10.11.43.29:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 91ms, Máximo = 976ms, Media = 322ms
```

Figura 8.8.10 Captura de trafico ICMP lanzado desde el portátil de pruebas para verificar la conectividad con el servidor de monitorización (10.11.43.29)

Comprobamos haciendo un traceroute el camino que sigue el datagrama IP desde la sede móvil al servidor de monitorización:

```
C:\>tracert 10.11.43.29

Traza a 10.11.43.29 sobre caminos de 30 saltos como máximo.

  1     1 ms    <1 ms    <1 ms  10.22.200.1
  2   851 ms  1249 ms   829 ms  172.26.204.2
  3  1341 ms  1079 ms   681 ms  10.11.43.29
Traza completa.
```

Figura 8.8.11 Captura de un traceroute lanzado desde el portátil de pruebas para ver el numero de saltos que emplea para alcanzar el servidor de monitorización (10.11.43.29) cuando se emplea túneles IPSEC.

Como se observa en la traza, **al emplear túneles IPSEC da la sensación que para alcanzar el servidor de monitorización es como si fuese una red punto a punto**, es decir, router de oficina móvil (10.22.200.1), router de la sede central (172.26.204.2) y el siguiente salto ya el servidor de monitorización. Si desaplicamos los túneles IPSEC en ambos routers y volvemos a generar un tracerouter el resultado es el siguiente:

```
C:\>tracert 10.11.43.29

Traza a 10.11.43.29 sobre caminos de 30 saltos como máximo.

  1     1 ms    <1 ms    <1 ms  10.22.200.1
  2  2886 ms   669 ms  1719 ms  10.21.34.33
  3     *        *        *     Tiempo de espera agotado para esta solicitud
  4     *        *        *     Tiempo de espera agotado para esta solicitud
  5   127 ms    89 ms    89 ms  10.128.248.1
  6   633 ms  1230 ms  1149 ms  172.26.204.2
  7   826 ms   899 ms    79 ms  10.11.43.29

Traza completa.
```

Figura 8.8.12 Captura de un traceroute lanzado desde el portátil de pruebas para ver el numero de saltos que emplea para alcanzar el servidor de monitorización (10.11.43.29) sin emplear túneles IPSEC.

En este caso se observa que da mas saltos para alcanzar el servidor de monitorización, en concreto 6 saltos, que corresponden a la oficina movil (10.22.200.1), POI pincipal (10.21.34.33), dos saltos en routers del backbone de la red IP Unica, el PE de la red Man de Madrid (10.128.248.1), y el router central (172.26.204.2).

8.11 Acceso al servidor de monitorización y visualizado del trafico generado

Para acceder al servidor de monitorización desde el portátil de pruebas bastara con abrir un navegador de Internet, y meter la url siguiente: **https://10.11.43.29/index.htm** tal y como muestra la captura:

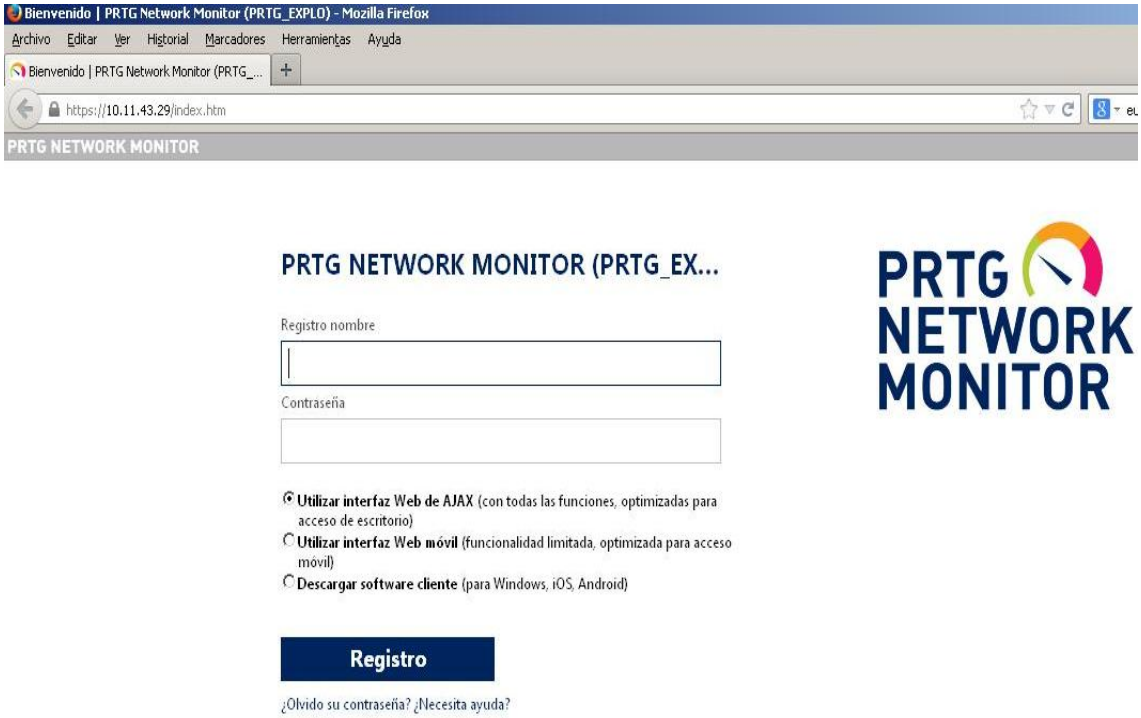


Figura 8.8.13 Captura de la pagina web de acceso al servidor de monitorización (10.11.43.29) para autenticarnos en el mismo.

Nos autenticamos y seleccionamos el la sonda que monitoriza los interfaces del router de la oficina movil. **Si generemos tráfico desde el portátil, por ejemplo, mediante un ping continuo con tamaño 6000 bytes**:

```
C:\>ping -l 6000 10.11.43.29 -t

Haciendo ping a 10.11.43.29 con 6000 bytes de datos:

Respuesta desde 10.11.43.29: bytes=6000 tiempo=287ms TTL=125
Respuesta desde 10.11.43.29: bytes=6000 tiempo=252ms TTL=125
Respuesta desde 10.11.43.29: bytes=6000 tiempo=231ms TTL=125
Respuesta desde 10.11.43.29: bytes=6000 tiempo=269ms TTL=125
Respuesta desde 10.11.43.29: bytes=6000 tiempo=279ms TTL=125
Respuesta desde 10.11.43.29: bytes=6000 tiempo=263ms TTL=125
Respuesta desde 10.11.43.29: bytes=6000 tiempo=268ms TTL=125
Respuesta desde 10.11.43.29: bytes=6000 tiempo=268ms TTL=125
Respuesta desde 10.11.43.29: bytes=6000 tiempo=269ms TTL=125
Respuesta desde 10.11.43.29: bytes=6000 tiempo=261ms TTL=125
Respuesta desde 10.11.43.29: bytes=6000 tiempo=278ms TTL=125
Respuesta desde 10.11.43.29: bytes=6000 tiempo=270ms TTL=125
Respuesta desde 10.11.43.29: bytes=6000 tiempo=240ms TTL=125
Respuesta desde 10.11.43.29: bytes=6000 tiempo=270ms TTL=125
Respuesta desde 10.11.43.29: bytes=6000 tiempo=241ms TTL=125
Respuesta desde 10.11.43.29: bytes=6000 tiempo=260ms TTL=125
Respuesta desde 10.11.43.29: bytes=6000 tiempo=250ms TTL=125
Respuesta desde 10.11.43.29: bytes=6000 tiempo=292ms TTL=125
Respuesta desde 10.11.43.29: bytes=6000 tiempo=240ms TTL=125
Respuesta desde 10.11.43.29: bytes=6000 tiempo=241ms TTL=125
```

Figura 8.8.14 Captura de trafico ICMP lanzado desde el portátil de pruebas contra el servidor de monitorización (10.11.43.29) para generar trafico a través del interfaz túnel 1 del router de la oficina móvil.

Veremos como en el **servidor de monitorización comienza a verse tráfico de entrada y salida a través del interfaz tunel1 del router de la oficina móvil**.

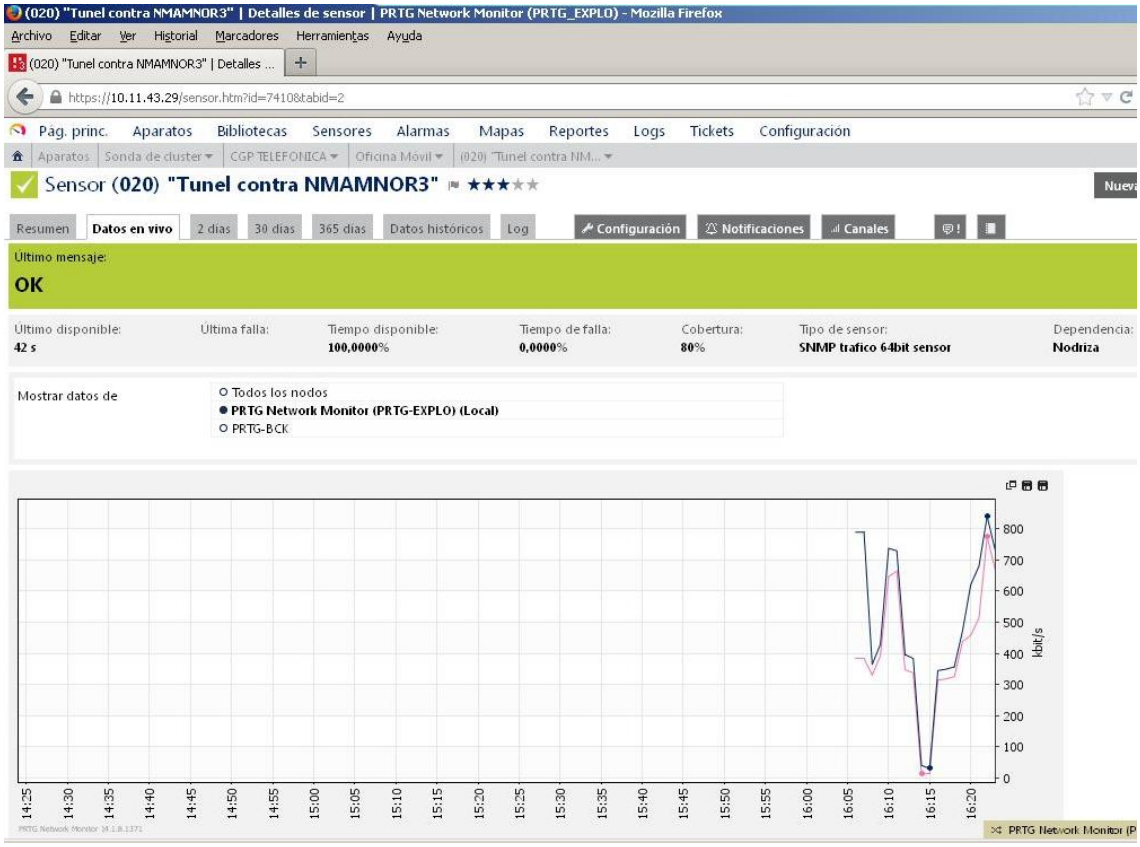


Figura 8.8.15 Captura de la pagina web del servidor de monitorización que muestra el trafico en tiempo real que se esta cursando en el router de la oficina móvil a través del interfaz túnel 1 contra el POI principal.

En el router mediante el **mandato show interface tunnel1 vemos el tráfico en bits/sec** que esta representado el servidor de monitorización en la grafica:

```
Oficina_Movil#sh int tunnel 1
Tunnel1 is up, line protocol is up
  Hardware is Tunnel
  Description: "Tunel contra NMAMNOR3"
```

```
Internet address is 10.21.34.34/30
MTU 17916 bytes, BW 100 Kbit/sec, DLY 50000 usec,
   reliability 255/255, txload 255/255, rxload 255/255
Encapsulation TUNNEL, loopback not set
Keepalive not set
Tunnel source 10.148.18.193, destination 172.19.136.61
Tunnel protocol/transport GRE/IP
  Key disabled, sequencing disabled
  Checksumming of packets disabled
Tunnel TTL 255, Fast tunneling enabled
Tunnel transport MTU 1476 bytes
Tunnel transmit bandwidth 8000 (kbps)
Tunnel receive bandwidth 8000 (kbps)
Last input 00:00:05, output 00:00:00, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 91
Queueing strategy: fifo
Output queue: 0/0 (size/max)
5 minute input rate 562000 bits/sec, 104 packets/sec
5 minute output rate 491000 bits/sec, 68 packets/sec
   120423 packets input, 79811697 bytes, 0 no buffer
   Received 0 broadcasts (0 IP multicasts)
   0 runts, 0 giants, 0 throttles
   0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
   93644 packets output, 70672274 bytes, 0 underruns
   0 output errors, 0 collisions, 0 interface resets
   0 unknown protocol drops
   0 output buffer failures, 0 output buffers swapped out
```

Para consultar el tráfico que pasa por los interfaces, **el servidor de monitorización emplea el protocolo snmp y ataca a la ip 172.29.29.200 que tiene configurada el router de la oficina móvil para realizar las consultas. Una vez obtenido el OID** lo representa en la grafica tal y como se puede ver en la traza obtenida en el router de la oficina móvil.

```
Oficina_Movil#show snmp mib ifmib ifindex
Loopback55: Ifindex = 22
ATM0.0-aal5 layer: Ifindex = 11
Loopback700: Ifindex = 23
```

Vlan20: Ifindex = 16

Tunnel2: Ifindex = 21

ATM0.0-atm subif: Ifindex = 9

ATM0-adsl: Ifindex = 12

Vlan19: Ifindex = 17

Loopback600: Ifindex = 15

Ethernet0-vdsl2: Ifindex = 13

ATM0-atm layer: Ifindex = 8

FastEthernet0: Ifindex = 3

FastEthernet2: Ifindex = 5

Virtual-PPP1: Ifindex = 18

Null0: Ifindex = 7

Ethernet0: Ifindex = 2

Tunnel1: Ifindex = 20

Vlan1: Ifindex = 14

ATM0-aal5 layer: Ifindex = 10

ATM0: Ifindex = 1

NVI0: Ifindex = 19

FastEthernet1: Ifindex = 4

FastEthernet3: Ifindex = 6

Apr 15 15:56:01.914 METDST: SNMP: **Packet sent via UDP to 10.7.43.29**

Apr 15 15:56:01.982 METDST: SNMP: **Packet received via UDP from 10.7.43.29 on Tunnel1**

Apr 15 15:56:01.986 METDST: SNMP: Get-next request, reqid 12725768, errstat 0, erridx 0

ifName.23 = NULL TYPE/VALUE

Apr 15 15:56:01.990 METDST: SNMP: Response, reqid 12725768, errstat 0, erridx 0

ifInMulticastPkts.1 = 0

Apr 15 15:56:01.994 METDST: SNMP: Packet sent via UDP to 10.7.43.29

Apr 15 15:57:08.998 METDST: SNMP: Packet received via UDP from 10.7.41.158 on Tunnel1

Apr 15 15:57:09.002 METDST: SNMP: **Get request, reqid 47027081, errstat 0, erridx 0**

ifAlias.20 = NULL TYPE/VALUE

ifHCInOctets.20 = NULL TYPE/VALUE

ifHCOutOctets.20 = NULL TYPE/VALUE

sysUpTime.0 = NULL TYPE/VALUE

Apr 15 15:57:09.018 METDST: SNMP: **Response, reqid 47027081, errstat 0, erridx 0**

ifAlias.20 = "Tunel contra NMAMNOR3"

ifHCInOctets.20 = 0x001332E53

ifHCOutOctets.20 = 0x00129DD06

CONCLUSIONES

En el contexto actual de las telecomunicaciones se ha pasado de centrar los análisis no solo en las infraestructuras y los terminales de los primeros años sino también en estudiar la adopción y uso cotidiano de las nuevas tecnologías que dan los ciudadanos. Las telecomunicaciones en el mundo actuales están caracterizadas por:

- Tendencia decreciente de la telefonía fija pero desacelera su crecimiento negativo.
- La telefonía móvil sigue aumentando pero en menor medida.
- La banda ancha crece en todo el mundo, tanto la fija como la móvil. Esta última supera ya a la fija en términos absolutos.
- Crece la facturación en las TIC sobre todo en las economías emergentes ya que en Europa sigue su economía en retroceso.

Respecto a Europa, las conclusiones del estado del mercado viene marcado por:

- La recesión y de ajustes severos en la Unión Europea (UE). Registró un crecimiento negativo del 0,5% y la actividad fue desacelerándose a medida que avanzó el año.
- Descendió la facturación global.
- Disminución de los ingresos por servicios de voz, tanto los prestados por redes fijas como los de redes móviles.
- Aumentaron los ingresos de banda ancha, sobre todo en el caso de la banda ancha móvil
- Por grado de penetración continua la tendencia de años posteriores ya que sigue descendiendo las líneas de telefonía fija, las de móvil crecieron aunque en menor medida y la banda ancha, en especial la banda ancha móvil que registro los datos más significativos de crecimiento.
- Sigue expandiéndose el servicio de VoIP en el hogar.
- La implementación de la Agenda Digital para Europa se estima que puede ayudar a incrementar un 5% el PIB de la UE.
- Las redes NGA fijas alcanzan a la mitad de los hogares de la UE y un buen número de operadores móviles de la UE iniciaron el despliegue y la implantación comercial de servicios de LTE, generalmente en las ciudades de tamaño medio y grande.

En España, no ajena a la crisis que vivimos, sus aspectos más relevantes son:

- Disminución de la facturación global del sector y de la inversión.
- Los operadores para combatir la crisis han disminuido los precios de los servicios como consecuencia de que están apostando decididamente por la convergencia de

sus distintos servicios de telecomunicaciones. Esto significa que a los clientes se les ofrecen ya servicios empaquetados en versiones de 4 play o 5 play, es decir, contratar todos los servicios (TV, móvil, fijo, banda ancha fija y móvil) con el mismo operador, supone un ahorro en los hogares. Este tipo de empaquetamiento está en crecimiento y que tuvo su origen en el producto Fusión comercializado por Telefonica y al que le han seguido el resto de operadores.

- La banda ancha móvil mantiene el crecimiento de la banda ancha y ya supera a la banda ancha fija.
- Sigue descendiendo los servicios tradicionales de voz, como es la telefonía fija, y por primera vez desciende también el número de líneas móvil como consecuencia principalmente de las numerosas bajas de tarjetas prepago.
- El Smartphone ya supera a los PC como dispositivos más vendido y en España es el cuarto país de la UE en tasa de penetración del Smartphone.
- Telefonica por debajo del 50% cuota mercado en banda ancha fija debido a que los operadores alternativos captaron mayor número de líneas fijas. Por el contrario, en los clientes de grandes cuentas, Telefonica sigue siendo el rey indiscutible en todos los servicios (fijo, móvil y banda ancha).
- Aumento considerable de las redes NGA debido a las inversiones realizas por Telefonica, es espacial crece FTTH y DOCSIS 3.0.
- La CMT ha aprobado un nuevo modelo de acceso indirecto llamado NEBA para los accesos de nueva generación ADSL2+, VDSL Y FTTH.

Referente a la adopción y uso de los usuarios que hacen de los dispositivos y las tecnologías las conclusiones obtenidas son:

- En las tecnologías de acceso a internet, la opción vía móvil ganan fuerza y complementan el acceso desde tecnologías fijas provocando que el dispositivo móvil se convierta en el motor de crecimiento de internet.
- El Smartphone se impone como el dispositivo más utilizado para conectarse en determinadas franjas horarias.
- Los Smartphone, tablets y ebook impulsan la modernización tecnológica de los hogares.
- El uso de otros dispositivos además del PC potencia el uso de redes y del pago por el acceso a contenidos.

- La navegación por Internet es el tipo de contenido accedido con mayor frecuencia y el más valorado. El acceso vía streaming supera definitivamente a la descarga de contenidos en el consumo de música y vídeo gracias a aplicaciones como Youtube o Spotify.
- Internet se posiciona como medio de comunicación preferido para comunicarse y convive con los demás medios más tradicionales. Respecto a la mensajería instantánea, Whatsapp sigue siendo el preferido de los usuarios.
- Continúa el crecimiento de las redes sociales, aunque el segmento de los más jóvenes pasa el relevo a los usuarios de edad media .Además, aumenta la frecuencia de uso de las redes sociales y las actividades que se realizan a través de ellas.

El futuro de las redes de telecomunicaciones pasa por desarrollar redes que tengan mayor flexibilidad y capacidad de ancho de banda ya el volumen de información a procesar crecerá exponencialmente en los próximos años. Para la alta capacidad se opta por las mallas fotónicas y las small cells y la flexibilidad y eficiencia aparece el concepto SDN que se trata de definir redes vía software, es decir, virtualizar redes tal y como ya se hace en la actualidad en los Data Centres.

Las infraestructuras de las redes del operador Telefonica se han tenido que adaptar al cambio de la convergencia entre datos y voz y fijo y móvil. En este proceso se encuentran las redes IP de Nueva Generación (NGN).La actual tendencia de integrar todo tipo de servicios en una única infraestructura de red IP ha puesto de manifiesto las carencias que tienen las soluciones IP clásicas en temas como la capacidad, la calidad de servicio, la seguridad o la fiabilidad. Tradicionalmente, las redes IP han sido la base del negocio de la transmisión de datos, manteniendo un aislamiento completo respecto a las redes de voz, basadas en una capacidad fija. Las redes IP tradicionales no están pensadas para transportar tráfico de voz, ya que éstas tienen unos condicionantes muy diferentes a los datos. Para solucionar estos problemas están los son los modelos de Red de Nueva Generación definida por Telefónica como un modelo de arquitectura de redes de referencia que debe permitir desarrollar toda la gama de servicios IP multimedia de nueva generación como son las comunicaciones VoIP, video comunicación, mensajerías integradas multimedia, integración con servicios IPTV o domótica. Las redes actuales de Telefonica está compuesta por:

1) Red IP Única

Nacida de la evolución de la red UNO-IP/NURIA la cual era de arquitectura compleja, baja capacidad de transporte y alta complejidad topológica, la cual estaba formada inicialmente tres redes IP desarrolladas verticalmente por cada una de las unidades organizativas (Residencial (RIMA), Empresas (RUMBA (Red Unificada Multiservicio Banda Ancha)) y Móviles (RUD (Red Unificada Datos)) y un conjunto de redes de circuitos especializadas en los servicios de voz fija y móvil que incorpora elementos de routing de alta conmutación, capaz de integrar los nuevos perfiles de tráfico IP y multimedia basado en "todo IP", y de soportar, eficazmente, la creciente demanda de servicios de acceso a Internet, tanto en banda estrecha (accesos conmutados) como, y especialmente, en banda ancha (ADSL), así como otros servicios multimedia sobre IP y Redes Privadas Virtuales IP. Diseñada, desplegada y habilitada para la prestación de servicios IP sobre cualquier tipo de acceso de cliente (Accesos por xDSL, RTC y accesos por líneas dedicadas punto-a-punto o Ethernet) buscando la escalabilidad y la calidad como objetivos clave de diseño de la red. Esta red es una de las de mayor capacidad de las existentes en la actualidad en España y una de las más modernas de la UE.Actualmente cerca del 75% del tráfico de Telefónica transcurre a través de la tecnología IP y la red IP Única queda compuesta por:

- Una red (RIMA) de altísima capacidad, disponibilidad, con tratamiento específico y diferenciado de los tráficos en función de su criticidad y abierto a Internet.
- Un anillo de conectividad crítica IP de alta capacidad y con alta seguridad estructural, blindado al mundo Internet y dedicado a soportar el tráfico sensible (con requisitos de gran disponibilidad) y altamente crítico para el negocio.

Según lo estudiado podemos concluir que sus características principales son:

- Arquitectura en red IP se basa en tres niveles (acceso, transito e interconexión) con elementos y rutas redundantes y equilibrado de carga con GigaRouters en el núcleo de red y con capas de gestión más simple.
- Posee una alta capacidad de transporte entre nodos mediante tecnología JDS (Jerarquía Digital Síncrona) y WDM (Wavelength-Division Multiplexing) y utilización de protocolo MPLS basado en el intercambio de etiquetas.
- Se emplean mecanismos de Clases de Servicio en los routers y servidores de acceso RAS y B-RAS.
- Fácil de implementar nuevas funcionalidades ya que su arquitectura está basada en productos comerciales y permite un mejor dimensionamiento de la red.

- Pensada para crecer y con avanzadas capacidades.
- Capacidad de soporte de RPV (Redes Privadas Virtuales basado en un modelo de acceso delegado sin túneles.
- El nivel de acceso está estructurado en zonas. Cada zona tiene un Centro de Acceso (CA). Los usuarios pueden acceder a la red a través de la red conmutada (RTB o RDSI) o a través de accesos dedicados ADSL. Los Centros de Acceso realizan la función de concentración de los usuarios, tanto conmutados como permanentes.
- Se tiene conectividad IP a redes externas con otros operadores de red de España (Vodafone,Orange….) con la red NGN y con redes internacionales.
- Con la red UNO o multiservicio se tienen conectividad para ofrecer los accesos Frame-Relay o ATM nativo a la red IP. Para accesos ADSL se ofertan a través de la Red GigADSL que tiene conectividad con la red multiservicio o directa con los centros de acceso de la red IP.
- La conectividad a nivel metropolitano/provincial se sustenta en la infraestructura asociada a la MAN.
- Ofrece entre otros, servicios RPVs IP como VPN-IP, Macrolan, DIBA, Acceso Intranet,Ibercom IP, Netlan.

2) Red UNO o Multiservicio

Es la evolución de la red Iberpac, se basa en tecnología ATM y Frame-Relay empleando equipos Passport de Nortel para realizar la conmutación de nivel 2 de las tramas. En el backbone de la red los equipos tienen una capacidad transmisión de hasta 2,5 Gb. Para el acceso a la red y concertación de servicios X.* también se emplean equipos DPN. La red ofrece conectividad multiprotocolo. Los accesos de los clientes pueden ser ATM, Frame-Relay, Ethernet, y también otros protocolos como X.25, X.28 y X.32. La red también sirve de acceso a clientes que conectan a la red IP Única.Permite conexiones permanentes (CVP) y conmutadas (CVC) extremo a extremo con utilización de direccionamiento IP público o privado, o de protocolos distintos de IP. Se basa en la creación de redes privadas virtuales tradicionales de nivel 2 con una infraestructura compartida por clientes manteniendo las mismas prestaciones que si fuera una red privada, reduciendo costes y aumentando rendimiento. Los servicios soportados sobre la red UNO se pueden clasificar en dos categorías en función de si se ofrecen sobre el nodo de red DPN o Passport:

- Bajo el nodo de red DPN se ofrecen los servicios de red tradicionales de IBERPAC que ya están prácticamente en desuso porque ya no se provisionan nuevos servicios bajo los DPN y los que existen se buscan emigrarlos a las nuevas arquitecturas de red bajo la Red IP Única. Son los Servicios X.25 (Iberpac, Iberpac plus), Servicio Datafono, Servicio UNO y Servicio FR
- Bajo el nodo de red PASSPORT sean servicios basadas en tecnologías FR o ATM. Son los Servicio FR, Servicio Interlan, Servicio Voz Interlan, Servicio ATM, Servicio CINCO,Servicio ViaSat y Servicio Nodo de Red.

3) Red NGN

La red NGN de Telefonica se fundamenta en la arquitectura NGN y en una estructura de control alineada con las especificaciones resultantes del 3GPP. Su arquitectura se basa en un modelo IMS el cual separa en niveles la funcionalidad de las soluciones extremo a extremo (end-to-end): Aplicaciones, Control, y Conectividad. De esta forma permite a cada nivel desarrollarse y evolucionar de forma independiente al resto, estando unos niveles condicionados más que otros, por el mercado y la evolución de la tecnología, como puede ser el caso de la migración en el nivel de conectividad a nuevas tecnologías de transmisión sin necesidad de que el resto de los niveles se vean afectados. Las principales entidades lógicas y físicas de la solución IMS residen en los niveles de aplicación y control, sin embargo entidades del nivel de conectividad son incluidos también en la solución con el fin de proveer una solución completa. Aunque la solución tiene por objetivo el ofrecer una amplia oferta de servicios de voz como AUIP,AAPPVV e Ibercom en RED y en un futuro aplicaciones multimedia, cuenta con unidades que permiten la interconexión con redes de circuitos tradicionales (RTC), PSTN mediante Gateways y con la Red IP Única mediante los SBC. Más adelante en el proyecto explicaré detalladamente el funcionamiento y servicios ofertados sobre la NGN.

4) Redes MAN

Se concluye que son redes diseñadas para proporcionar conectividad de banda ancha basadas en el trasporte de tráfico Ethernet entre redes de área local de los clientes ubicados en lugares diferentes de la misma provincia o con los routers de acceso de la red IP Única para las comunicaciones interprovinciales. Se trata de una red multipunto dividida en dos niveles, de acceso y agregación. Además se ofrecen diferentes calidades de servicio. Utiliza

multiplexación de conexiones sobre un mismo puerto físico según el protocolo 802.1Q o VPLS.

5) Redes de acceso para líneas fijas con arquitectura XDSL, FTTH

Las redes de Acceso de Banda Ancha de Telefónica para líneas fijas basadas en tecnología XDSL y FTTH presentan 3 arquitecturas diferenciadas bajo el nombre de tres redes: GigADSL, Alejandra y Red 50.

- GigADSL: es un servicio de nivel 2, para bucles de abonado indirectos basado en el establecimiento de un PVC ATM entre el usuario y el PAI (Punto de Acceso Indirecto) local del operador que contrate el servicio. El acceso se compone de un bucle de abonado de par de cobre basado en tecnología ADSL con un modem en el domicilio del cliente ATU-R y otro en central ATU-C. El backbone se compone de un tramo ATM hasta un punto de interconexión, donde se concentran todos los accesos de una determinada zona geográfica. Este punto de interconexión o PCC es recibido en un Passport de la Red Multiservicio que hace las funciones de red de agregación donde los PVC de ATM se encaminarán hacia el router de acceso de la Red IP Única pertenecientes a los CA.
- Alejandra: basada una arquitectura Ethernet pensada para ofrecer servicios de VoIP, TV e Internet donde la red GigADSL no dispone de los mecanismos para soportar estos servicios. Básicamente la red Alejandra está pensada para el servicio Imagenio de Telefonica sobre accesos con tecnología ADSL2+ y VDSL2 sobre par de cobre que se multiplexan en DSLAM IP. Utiliza mecanismos de calidad de servicio QoS para priorizar el tráfico de Voz. La conexión troncal que une los DSLAM IP a la red Ethernet se comparte entre todos los servicios diferencias por Vlanes.
- 50: red de acceso en el ámbito de las ciudades más importantes, cuyo objetivo es aumentar la cobertura de la red de acceso ofreciendo capacidades de hasta 100 Mbps al 60% de hogares españoles para poder ofrecer los servicios de Imagino con calidad. La tecnología empleada se basará en acercar la fibra óptica (FTTH) al usuario basada en tecnología GPON.

6) Redes de acceso para líneas móviles con arquitectura GSM/GPRS/UMTS/LTE

Para el tráfico de acceso de las líneas móviles se emplean las redes basadas en la arquitectura GSM/UMTS y la nueva LTE. El transporte para el transporte de tráfico 2G se apoya en la red ATM con cobertura geográfica nacional por medio de circuitos dedicados E1´s de la red de transmisión SDH y en las redes MAN para los datos 3G.

La oficina móvil empleada para conectarse a un servidor de una intranet utiliza el servicio vpn-ip de Telefonica que lo que permite es la interconexión de redes locales sobre infraestructura IP (con tecnología MPLS) acercando los usuarios desplazados a su sede central. Gracias a la tecnología MPLS, permite separar los tráficos de distintos clientes que viajan por la Red IP Única, proporcionando los mismos niveles de seguridad que los ofrecidos sobre redes tradicionales (FR/ATM).

La oficina movil al emplear acceso basado en tecnologia 3G proporciona las siguientes ventajas:

- El equipamiento se puede utilizar donde Telefónica no tiene cobertura fija (ya sea fibra óptica o par de cobre).
- Para la apertura de una delegación y por problemas o retrasos en la provisión del servicio no se llega a tiempo con la infraestructura fija, por tanto, la puesta en marcha de la infraestructura es resulta con mayor brevedad.
- Para empresas donde la oficina es durante un tiempo de duración determinada, como ejemplo, podríamos tener una caseta de obra y donde el coste de tirada de líneas para darse al tiempo de baja es más costo que la solución de acceso móvil.
- Se pueda utilizar también como respaldo de un acceso principal (ADSL o Ibermic) en caso de caída de esta línea.

El emplear una antena Ethernet no integrada en el router cisco proporciona la obtención de una mejor cobertura radio al poder situar la antena alejada del router y buscar el mejor sitio de cobertura dentro de la oficina ya que la existencia de obstáculos físicos entre esta y la estación base, degradan la señal inalámbrica lo que implica que afecten al rendimiento y las prestaciones del servicio aumentando la latencia, jitter y retardos en el tráfico generado a través de la oficina móvil. El uso de un inyector POE se concluye que:

- Permite instalaciones más sencillas y estéticas al precisarse sólo de un cable a la Antena.

- Se prescinde de la fuente externa de alimentación.
- Deja de ser necesario que haya un enchufe junto al módem.

Para que funcione el acceso móvil es necesario que el ICC y el MSISDN se provisione correctamente en el APN del cliente que corresponda ya se requiere que este dado de alta en la base de datos de LDAP para que luego el radius le diga al GGSN que ip se ha de incluir en el router para el establecimiento de los túneles GRE.

Respecto a la configuración empleada de opción 43 de DHCP es debido a que la antena teldat UMTS solo admite como parámetro la cadena de validación DHCP ("antenna") para el paso de parámetro IP y de acceso a la red 3G.

Debido a que los túneles GRE no mandan keepalive para saber si están operativos debido a que los POI de la marca Juniper no lo soportan es necesario empleado el routing dinámico BGP para detectar las caídas de los túneles, creando dos sesiones de BGP, una para el POI principal y otro para el backup. El direccionamiento LAN que se ponga en la oficina móvil y que se publicara por routing BGP no deberá existir en la tabla de rutas de la vrf de Caser puesto que existiría un solapamiento del direccionamiento. GRE es un protocolo que puede encapsular una amplia variedad de tipos de protocolos diferentes dentro de túneles IP, creando una red punto a punto entre el router de la oficina móvil y los POIs y no dependiendo de los protocolos que corren por debajo en la red de móviles.

Para dotar de cifrado al tráfico que se cursa por acceso 3G y evitar que vaya el flujo de datos en claro, el túnel IPSEC estático asegurar las comunicaciones sobre IP autenticando y/o cifrando cada paquete IP. El cifrado que se configurara será en modo túnel, es decir, todo el paquete IP (datos más cabeceras del mensaje) es cifrado y/o autenticado. Por tanto, debe ser entonces encapsulado en un nuevo paquete IP para que funcione el enrutamiento. El modo túnel se utiliza para comunicaciones red a red o comunicaciones ordenador a red u ordenador a ordenador sobre una red insegura. El empleo de IPSEC hace que para los equipos que están detrás la red sea vista como una red punto a punto entre los dispositivos que participan en el túnel. Para que el túnel IPSEC se establezca es necesario que se genere tráfico que cumpla las condiciones de cifrado.

El servidor de monitorización es capaz de obtener la información del trafico que pasa por los interfaces del router de la oficina móvil empleando el protocolo de snmp que realiza consultas al objeto en concreto, pero no solo se limita a consultas, ya que podría recibir alarmas en caso de suceder algún evento, como podría ser la caída de un interfaz lo que da un mayor supervisión y control de lo que se esta monitorizando.

REFERENCIAS BIBLIOGRÁFICAS

(1) CTNE y Telefonica de España (años 1924-1935 y 1939-2011); Memorias. Compañía Nacional Telefónica de España.

(2) CMT (1998-2004); Informes anuales. Comisión del Mercado de las Telecomunicaciones.

(3) Fundación Telefonica (2010-2012). Informes Anuales. La sociedad de la Información. Telefonica de España.

(4) CMT (2008-2012); Informes anuales. Comisión del Mercado de las Telecomunicaciones.

(5) Eurobarometer (2012); 'Consumers' attitudes towards cross-border trade and consumer protection.

(6) GFK (2012); Análisis del mercado de Ebooks y Readers en España.

(7) Google (2012); Our Mobile Planet: Global Smartphone Users.

(8) IAB Spain Research (2012); Hábitos y Usos de Webs de compra Flash Sales.

(9) Fundación Orange (2010-2012).Informes Anuales. eEspaña 2012. France Telecom.

(10) ONTSI, Red.es (2010); Estudio sobre Comercio electrónico B2C 2010. El Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información.

(11) ONTSI, Red.es (2010-2012). Informes Anuales. La Sociedad en Red. El Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información.

(12) ONTSI, Red.es (2010-2012). Informes Anuales. Contenidos Digitales en España. El Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información.

(13) ONTSI, Red.es (2010-2012). Informes Anuales. Las TIC en los hogares españoles. El Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información.

(14) ITU (201-2011).Informes Anuales. Estadísticas sobre el sector TIC. International Telecommunication Union.

(15) AIMC-EMG (2012); Audiencia de Internet en la EGM.

(16) AIMC-EMG (2011); Navegantes en Red.

(17) Asimelec (2011); Informe 2010 industria contenidos digitales.

(18) Asimelec (2012); Informe del macrosector TIC en España.

(19) AMETIC (2011); El hipersector TIC español 2010

(20) AMETIC (2011); Las tecnologías de la información en España.

(21) AMETIC-Accenture (2011); Retos y oportunidades del universo digital móvil en España: más ubicuo, más social, más personal.

(22) Telefonica de España (2003); Servicio RPV-IP en RIMA. Proyecto Técnico de Explotación impactos en RIMA. Dirección de Tecnología.

(23) Telefonica de España (2002); Proyecto Técnico de la red RIMA. Dirección de Tecnología.

(24) Telefonica de España (2008); Plan técnico de integración RIMA-RUMBA. Área de estrategia y desarrollo de la red.

(25) Telefonica de España (2012); Plan técnico de evolución de núcleo e interconexión de red IP 2013-2014. Área de planificación y tecnología.

(26) Telefonica de España (2012); Plan técnico de evolución del anillo para la conectividad crítica IP. Área de estrategia y desarrollo de la red.

(27) Telefonica de España (2008); Estructura de red del nivel de transito del anillo para la conectividad critica IP. Área de estrategia y desarrollo de la red.

(28) Telefonica de España (2011); Criterios de diversificación de enlaces del anillo IP para la conectividad crítica. Área de estrategia y desarrollo de la red.

(29) Telefonica de España (2010); Criterios de dimensionado y calidad de servicio (Qos) en el anillo IP para la conectividad critica. Área de estrategia y desarrollo de la red.

(30) Telefonica de España (2010); Estructura de los centros de acceso del anillo. Área de estrategia y desarrollo de la red.

(31) Telefonica de España (2007); Plan técnico de RUD. Área de estrategia y desarrollo de la red.

(32) Telefonica de España (2008); Plan técnico de red IP móvil (RUD). Área de estrategia y desarrollo de la red.

(33) Telefonica de España (2009); Cambio conexión RUD-RIMA. Área de estrategia y desarrollo de la red.

(34) Telefonica de España (2011); Estructura de red PCRF. Área de estrategia y desarrollo de la red.

(35) Telefonica de España (2011); Plan técnico de evolución 2009-2010-2011 de los centros de red de banda ancha (CERBA) de RIMA. Área de estrategia y desarrollo de la red.
(36) Telefonica de España (2011); Especificación de requisitos de nuevos servicios de Internet en Red Única. Área de estrategia y desarrollo de la red.
(37) Telefonica de España (2009); Estructura de referencia de comunicaciones de gestión de activos de red proyección gestión de red móvil. Área de estrategia y desarrollo de la red.
(38) Telefonica de España (2011); Plan técnico de evolución de la red ATM de servicios móviles 2012-2013. Área de estrategia y desarrollo de la red.
(39) Telefonica de España (2012); Documento de requisitos para transporte en el backhaul de LTE. Área de desarrollo redes acceso agregación y transporte.
(40) Telefonica de España (2011); Plan técnico de evolución del transporte de la red móvil MTS 2013-2014. Área de desarrollo redes acceso agregación y transporte.
(41) Telefonica de España (2011); Plan técnico de evolución de los centros de acceso residencial IP 2011-2012. Área de estrategia y desarrollo de la red.
(42) Telefonica de España (2011); Plan inicial de integración de servicios "línea ADSL" sobre la arquitectura Alejandra. Área de estrategia y desarrollo de la red.
(43) Telefonica de España (2011); Nodos ATM de CISCO perfiles servicio GigADSL. Área de estrategia y desarrollo de la red.
(44) Telefonica de España (2011); Plan técnico de despliegue de MGX 8850. Área de estrategia y desarrollo de la red.
(45) Telefonica de España (2007); Arquitectura de red para GPON en Alejandra. Área de estrategia y desarrollo de la red.
(46) Telefonica de España (2005); Arquitectura del acceso y de la red metropolitana para la red 50. Área de estrategia y desarrollo de la red.
(47) Telefonica de España (2010); Manual técnico del servicio Macrolan. Área de soluciones tecnicas de datos.
(48) Telefonica Data de España (2011); Manual técnico del servicio VPN-IP. Dirección de Planificación y Desarrollo técnico de Servicios. Subdirección de Servicios de RPV. Área de soluciones técnicas de datos.
(49) Telefonica Data de España (2007); Acceso a Intranet. Descripción Técnica del servicio en Modalidad Privada. Dirección de Planificación y Desarrollo técnico de Servicios.
(50) Telefonica Data de España (2008); Acceso a Intranet. Descripción Técnica del servicio en Modalidad Publica. Dirección de Planificación y Desarrollo técnico de Servicios.

(51) Telefonica Empresas (2010); Acceso a Intranet. Manual Técnico del servicio Datainternet IPv6. Dirección de Planificación y Desarrollo técnico de Servicios.

(52) Telefonica de España (2005); Manual Técnico Nuevos Accesos ATM para Interlan. Configuración en red Multiservicio. Dirección de Planificación y Desarrollo técnico de Servicios.

(53) Telefonica de España (2011); Especificaciones técnicas servicio Ibercom IP. Dirección de Planificación y Desarrollo técnico de Servicios.

(54) Telefonica de España (2010); Especificaciones técnicas servicio Netlan. Dirección de Planificación y Desarrollo técnico de Servicios.

(55) Telefonica de España (2010); Estructura de red para la migración del núcleo de la red NGN dede red IP Única a anillo critico. Área de estrategia y desarrollo de la red

(56) Telefonica de España (2011); Estructura de red para el despliegue del servicio CANGN basado en arquitectura IMS/NGN. Área de estrategia y desarrollo de la red

(57) Telefonica de España (2012); Descripción técnica del servicio integración servicio Ibercom IP en red NGN. Área de estrategia y desarrollo de la red

(58) Fernandez-Palacios, J.P (2013); Redes de transporte elásticas. Telefonica I+D área de Estrategia de Negocio y Tecnológica.

(59) Ramon, F.J. (2013); SDN World 2013. Asomándonos a la red Del futuro. Telefonica I+D área de Estrategia de Negocio y Tecnológica.

(60) Lopez, D.R. (2013); SDN, un cambio de paradigma llega a las redes. Telefonica I+D área de Estrategia de Negocio y Tecnológica.

(61)http://materias.fi.uba.ar/7543/download/conf_gre.pdf

(62)http://librosnetworking.blogspot.com.es/2006/12/introduccin-tneles-gre.html

(63)http://www.tecnun.es/asignaturas/redtelema/Guion%20practica%206%20VPN.pdf

(64)http://www.net130.com/technic/ciscotech/config%20virtual%20template%20interfaces.pdf

(65) http://www.iit.upcomillas.es/pfc/resumenes/4fc8ba45f40fe.pdf

(66) Telefonica de España (2012); Antena Ethernet. Formacion sobre la instalacion en Servicios de Empresas v1.5. Área de estrategia y desarrollo de la red

(67) Telefonica de España (2012); MT, Acceso MS Intranet a RPVs & Accesos y Respaldos Moviles para VPNIP e Interlan.Area de tecnologia y desarrollo de servicios